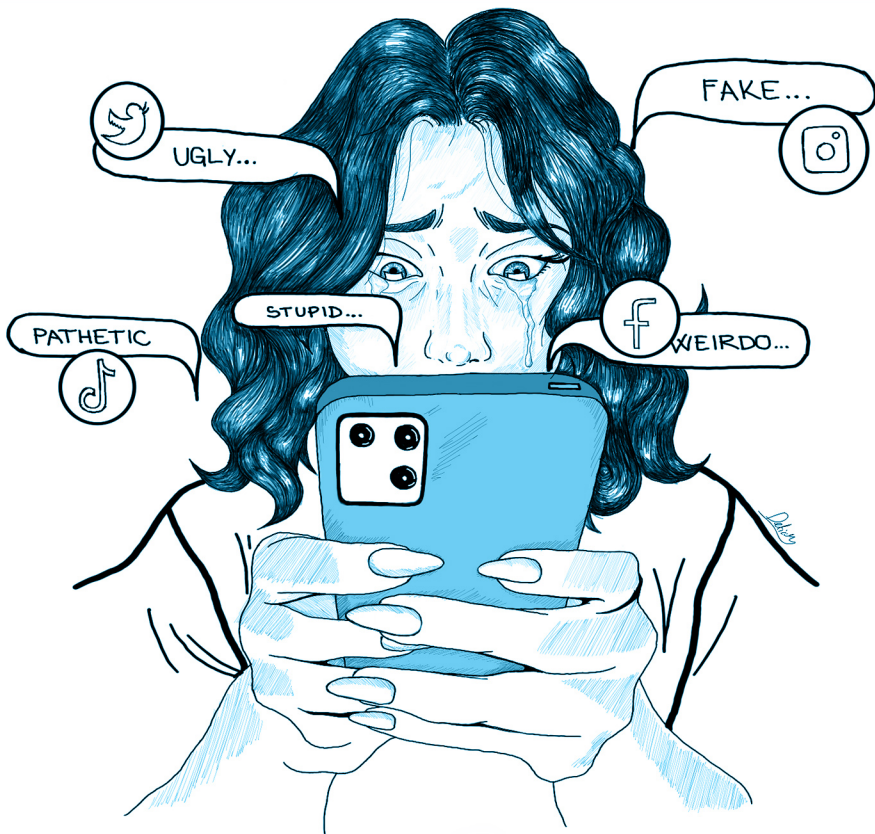




University of Maribor Press

CYBER SECURITY



edited by

Tatjana Welzer Družovec

**Training Students and Scholars for the
Challenges of Information and
Communication Technologies in
Research and Studies for
Internationalisation**

HANDBOOK



**Cyber Security - Training Students and Scholars for the
Challenges of Information and Communication
Technologies in Research and Studies for
Internationalisation**

Handbook

Editor
Tatjana Welzer Družovec

April 2023

- Title** **Cyber Security - Training Students and Scholars for the Challenges of Information and Communication Technologies in Research and Studies for Internationalisation**
- Subtitle** **Handbook**
- Editor** Tatjana Welzer Družovec
(University of Maribor)
- Review** Michel Labour
(Université Polytechnique de Haute-de-France)
- Tobias Baumeister
(Brandenburg Technical University)
- Céline Faure
(Université Polytechnique de Haute-de-France)
- Language editing** Mladen Kraljić
(University of Maribor)
- Stojan Primožič
(University of Maribor)
- Technical editor** Jan Perša
(University of Maribor, University Press)
- Cover designer** Jan Perša
(University of Maribor, University Press)
- Cover graphic** Cyber Crime, author: Ajda Detiček, 2023
- Published by** **University of Maribor**
University Press
Sloški trg 15, 2000 Maribor, Slovenia
<https://press.um.si>, zalozba@um.si
- Publication type** E-book
- Available at** <http://press.um.si/index.php/ump/catalog/book/753>
- Published at** Maribor, Slovenia, April 2023



© University of Maribor, University Press
/ Univerza v Mariboru, Univerzitetna založba

Text © authors, Welzer Družovec 2023

This work is licensed under the Creative Commons Attribution 4.0 International License.

This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The license allows for commercial use.

Any third-party material in this book is published under the book's Creative Commons licence unless indicated otherwise in the credit line to the material. If you would like to reuse any third-party material not covered by the book's Creative Commons licence, you will need to obtain permission directly from the copyright holder.

<https://creativecommons.org/licenses/by/4.0>



Project name Cyber Security - Training Students and Scholars for the Challenges of Information and Communication Technologies in Research and Studies for Internationalisation

Project number 2020-1SI01-KA203-075893

Project financier European Union's Erasmus+

“The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein”



ATHENA

CIP - Kataložni zapis o publikaciji
Univerzitetna knjižnica Maribor

004.056:004.738.5(076)

CYBER Security- Training Students and Scholars for the Challenges of Information and Communication Technologies in Research and Studies for Internationalisation [Elektronski vir] : handbook / Tatjana Welzer Družovec. - Maribor : Univerza v Mariboru, Univerzitetna založba, 2023

Način dostopa (URL): <https://press.um.si/index.php/ump/catalog/book/753>

ISBN 978-961-286-693-8

doi: 10.18690/um.1.2023

COBISS.SI-ID 140368387

ISBN 978-961-286-693-8 (pdf)
978-961-286-698-3 (hardback)

DOI <https://doi.org/10.18690/um.1.2023>

Price Free copy

For publisher Prof. Dr. Zdravko Kačič
Rector of University of Maribor

Attribution Welzer Družovec, T. (ed.) (2023). *Cyber Security - Training Students and Scholars for the Challenges of Information and Communication Technologies in Research and Studies for Internationalisation: Handbook*. Maribor of Maribor, University Press. doi: 10.18690/um.1.2023

Table of Contents

Information Security Management in Organisational Settings and Higher Education Institutions Kaja Prislan	1
Cybersecurity for Online Education Marko Kompara, Marko Hölbl	45
Protection of Personal Data (Guidelines for Educational Institutions and Students) Aljoša Polajžar	65
Labour Law and Cybersecurity in Higher Education Klemen Drnovšek	95
Human Rights and Cybersecurity Rok Dacar	105
Copyright Protection in Education Kristijan Zahrastnik	117
Cybercrime and Computer-related Offences Jan Stajko, Oskar Peče	133
Moodle Basics – A User Guide Mariusz Głabowski, Jakub Grzelski, Konrad Śniatała Paweł Śniatała, Michał Weissenberg	143

INFORMATION SECURITY MANAGEMENT IN ORGANISATIONAL SETTINGS AND HIGHER EDUCATION INSTITUTIONS

KAJA PRISLAN

University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia
kaja.prislan@um.si

Abstract In modern times, marked by trends in digitalisation, e-commerce, and the use of advanced technological solutions on the one hand and increasingly common and dangerous information threats on the other, information security management and information incident prevention have become crucial for successful and efficient organisational performance. This chapter presents the basic concepts and approaches to information security management in organisational settings and the core factors and contemporary trends that affect information security risks. Special emphasis is placed on the review of information security in higher education institutions, which are particularly exposed to cyberthreats due to their specific activities, culture, and values.

Keywords:

information security, information risk, management, organisations, higher education institutions

1 Introduction

Digitalisation, e-commerce and communication, and the development of advanced technological solutions, belong among the most actual trends of modern times, causing drastic changes in the security field at the same time. Although the performance of various activities has been simplified and enhanced (as there are communication, socialisation, learning, data management, business and decision-making), there is also the phenomenon of new security risks.

The main side-effect of technological development and progress are information threats and cybercrime, strongly influencing changes in traditional pre-conditions for providing security and privacy. In the 21st Century, threats of that kind gained unimaginable dimensions. Cyberthreats representing a rarity a decade ago, are a daily thing in contemporary times. At the same time, they constantly develop further and become more and more organised, sophisticated and unpredictable. A challenge exists mainly because such crimes do not know for geographical or other borders and cause severe damage to individuals, as well as to organisations and countries throughout the world.¹ Due to the hidden nature of actions by criminals, cyberthreats are difficult to recognise, as they might perform undiscovered in a system (or abuse a system and its data, respectively) for a longer time. At a particular moment, they might disable critical processes and systems. Due to its unpredictable and hardly manageable nature, cybercrime has become the main security problem of contemporary times (*EU Security Union Strategy, 2020; Interpol, 2021*). In line with growing threats caused by cybercrime and threats connected to privacy and personal data protection, in 2020, a new *EU Cybersecurity Strategy for the Digital Decade* was adopted. In the strategy, as one of the key challenges of the EU, a lack of collective awareness of cyberthreats is stressed, and among the goals belong efforts to establish joint capacities for reaction to cyberattacks, development of organisational capacities and technical protection as well as regulation of behaviour and privacy in the internet.

¹ According to assessments of security organisations, cyber-crime causes a damage of approximately six billion dollars or more than five billion Euros on an annual base (Morgan, 2020; The EU's Cybersecurity Strategy for the Digital Decade, 2020), while interferences into political processes are threatening also the pillars of democracy (Lažići, 2019).

Most negative effects of digitalisation and technological development are faced mainly by organisations and subjects of commerce (European Crime Prevention Network, 2016). The newest data show that in Europe, each eighth enterprise has been a victim of a cyberattack already (Eurostat, 2020), and there are multiple reasons for that. Organisations support their success or development, respectively, with different technological solutions that have a double role in the commercial surrounding; they are a source of competitiveness and numerous security vulnerabilities. In the same way, organisations managing a growing number of data is the primary goal of committers of cybercrime. Namely, in the world of commerce, information is the most important capital and source of power and, consequently also a very much searched good (Furnell & Moore, 2014). The main advantage of information and communication technology [ICT] and information systems for organisations lies within the improvement of the effectiveness of commerce and decision-making, but because information systems save vast amounts of personal data and other relevant information (e. g. intellectual property and business secrets) they also became exposed and when protected the most vulnerable point in an organisation's structure insufficiently, because of numerous vulnerabilities and simple possibilities of abuse.

Therefore, the concept of organisational security has strongly changed by moving organisations into cyberspace. Compared to other forms of threats, information or cyberthreats create specific risks, because of which the system of organisational security gained a new dimension. Information systems created a unique environment within an organisation composed of its most valuable assets. At the same time, they created a new entry point into the organisational structure, through which all other physical and technical security measures may be circumvented. When organisational security could be taken care of only by technical and physical protection are over (Prislán & Bernik, 2019).

Numerous well-known cases of hacker attacks, intrusions into information systems, identity thefts, disclosure of personal data, espionage and trade with business secrets that we witnessed in the past years prove that the stability and success of commerce in the information era is strongly depending on the capability to manage information security risks and to provide for information security. Although practically every organisation may be the target or victim of an information incident, certain branches (e. g., health, finances, production, high-tech, education, governments, energy or

critical infrastructure) are stronger exposed to such kinds of risks due to their sensibility and number of confidential data managed by them.

Providing information security represents a substantial managerial challenge. Despite the negative influence of information incidents on organisational security, systematic and strategic management of this field is merely in a developmental phase in many organisations. Recently, progress and development were to be noted in the field of organisational practice, but threats develop essentially faster than organisations can follow. A major challenge lies within the fact that information security is a complex system to be handled by a plan systematically on a multilayer and multidimensional level.

This chapter aims to present basic concepts of information security management, i. e., key aspects and steps relevant to the establishment of a successful approach to providing information security in organisations, and actual trends in the field of cyberthreats and information security risks. There, special emphasis is placed on the state and management of information security in higher education institutions. Namely, the education branch, due to its nature and culture and growing digitalisation and distance education, in the scope of cybercrime and information threats, belongs among the most exposed and vulnerable branches (Alexei, 2021; Check Point, 2022).

2 Development of the Information Security Discipline

The vast expert discussions and research activity of the past two decades led to a better understanding of the complex nature of information security and the development of scientific cognitions in this discipline. Approaches to providing information security developed parallel to the development of ICT, but views on the security of information systems were oriented towards technical aspects and mechanisms at the beginning (Whitman in Mattord, 2012; Von Solms, 2010). Due to this, the development of information security discipline ran slower than the development of threats and crimes in this field in practice.

Due to expert assessments, information security as a discipline started to develop intensively after the year 2000. Till the middle of the 90s of the past century, mainly IT experts dealt with such aspects, and attention was directed towards basic technical protection. Later, views on security and privacy changed or were upgraded; respectively, information security exceeded traditional frames and gained the mark of an interdisciplinary science (Anderson & Moore, 2009; Hommel, Metzger, & Steinke, 2015).

Development of information security through time may be comprised of five larger periods that differ regarding the aspects that were developed in that time and were exposed as a priority in the providing security of information and information systems (von Solms, 2010). The first period is called the *technical wave*, which lasted till the 80s of the past century. In this period, simple technical measures were developed (e. g., identification and authentication procedures), and questions of security were usually dealt with by technicians or computer experts, respectively. The second period or the so-called *management wave* ran till the middle of the 90s. During this time, policies intensively started to develop, procedures were prescribed, special organisational departments were established, and specific responsibilities for information security were trusted to managers or the leadership level. The reason laid within the phenomenon of a growing number of interconnected technologies in networks and the distribution of data. The *institutional wave*, or the third period, lasted till about the year 2005. This period was marked by the cognition those information threats may have severe consequences for organisations. By this, the convincement prevailed that the approach to providing information security has to be inter- and multidisciplinary. Information security has become increasingly the responsibility of strategic management and an important part of organisational culture. For the fourth period, named the *information security governance wave* that started in 2005, the development of different standards and stronger warnings to the management to take responsibility for the management of information security risks is characteristic. By 2006, almost parallel to the fourth period, the fifth period or the so-called *cybersecurity wave*, started. After this milestone, concepts of protection and management were upgraded as a consequence of a growing inclusion of organisation in cyberspace, a growing digitalisation and the phenomenon of more and more organised and sophisticated threats and attacks.

Based on the development of cognitions and different views on the nature of information security and information threats, also definitions of information security gradually developed. Today, the most frequent and established definition used by different international and expert organisations is that information security refers to the protection of information and information systems from unauthorised access, use, disclosure, defect, change or destruction with the aim of guaranteeing its *confidentiality, integrity and availability*. (ISO/IEC 27000:2018; Nieleš et al., 2017). Thus, it is about a system of security or protective measures and mechanisms to provide for three intervening target states formed by the so-called *CLA triad* – a model of attributes of information security established in the field (*confidentiality, integrity, availability*).

For confidential, personal data and information with a high value, confidentiality is an extraordinarily relevant security aspect. Providing for confidentiality refers to the prevention of unauthorised disclosure of information. The condition of confidentiality is met when information is protected from disclosure or unauthorised insight, and only users with proper access rights with a purpose have access. Confidentiality is connected to the concept of mystery and privacy, meaning that information remains hidden or covered and inaccessible for all people and services without being granted access. The most frequent measures of providing confidentiality are encryption or coding of data and communication, security classification of information, systems of registration and prevention of intrusion (IDS/IPS), antivirus programmes, management with access and user rights, the definition of responsible persons and their responsibilities as well as awareness of users on legitimate use (Osborne, 2006; Pfleeger & Pfleeger, 2006; Seese, 2009; Whitman & Mattord, 2012).

The criterion of *integrity* refers to the providing for quality of information. This means that information can be trusted or was changed or processed only by authorised persons. Consequences of loss of integrity are incorrect, false or unreliable information that may lead to wrong decisions. Providing for integrity includes verifying credibility and protecting information from unallowed changes and their integrity. The main measures fitting this criterion are following the revision trail, access control, user rights management, verification of thickening value and trust-building (Boersma, Loke, Petkova, Sander, & Brombacher, 2004; Osborne, 2006; Pesante, 2008; Pfleeger & Pfleeger, 2006; Whitman & Mattord, 2012).

Availability is a condition meaning that information and systems are available whenever authorised users need them. The main characteristics of availability are system accessibility, reliability and appropriate permeability of a system (ISO/IEC 27000:2018; Nieves et al., 2017). Availability is tightly connected to the reliability of the functioning and capacity of information systems, and measures attempt to prevent loss of information, defects, unavailability or degradation of information systems. Among the most frequent measures of providing for availability belong antivirus programmes, security copies, doubling critical parts of information systems, use of reliable infrastructure and proper maintenance, network surveillance, systems for detection and prevention of intrusion (IDS/IPS), reaction plans for incidents and resilience (Nieves, Dempsey, & Pillitteri, 2017; Osborne, 2006; Pesante, 2008; Whitman & Mattord, 2012).

By the described attributes or criteria of information security, some other phenomena relevant to be respected and achieved in a system of information security are connected. These are (Whitman & Mattord, 2012): (a) accuracy connected to integrity and referring to reliability and flawlessness of information and guarantee for an expected value; (b) authenticity likely connected to integrity, but referring to quality and legitimacy, which means that data are authentic, original and trustworthy or do not contain harmful elements; (c) utility connected to availability, but meaning that data is properly formatted, presented or saved and have a value for use at work or decision-making to the user; (d) possession is connected to the criterion of confidentiality and refers to the request that the use of a system and data processing is controlled by owners or caretakers with the intension to provide for proper supervision, overview and traceability of activities and events of information use. Also, Ulven & Wangen (2021) state in a similar context that the CIA triad has to be upgraded, i. e. by concepts, as there are: privacy, identification, authentication, authorisation and accountability.

Thus, today information security is not just a technical question, but a complex, multidimensional field composed of a *social and technical sub-system*. This means that information security is influenced by organisational, human, as well as by technological factors (Prislan, Mihelič, & Bernik, 2020). When planning the mere approach and measures, besides the described attributes or criteria, organisations must understand the role or function of information security in the organisational environment, as well. A relevant role of information security is providing for an

uninterrupted activity (i. e., providing for the capability of uninterrupted functioning of information systems despite a potential event and incident) and *information security risk management* (i. e. providing for a state of acceptable risks or minimum risk). Despite the importance of information security for commercial success, in the building of this, one must also respect the needs for rationality, economy and flexibility. Namely, it is impossible to provide absolute security, as all risks cannot be predicted or even addressed in a meaningful way.

3 Relevance of Information Security in the Organisational Context

In practice, within organisations, there are frequently questions regarding the relevance of information security and the need for investment in the mentioned field. The reason for this is a lack of tangible profitability of investments in information security, as security measures are aiming at a reduction of losses and not at common creation of profit (Schatz & Bashroush, 2017). Since security is a field without direct financial income, sceptical views on investments are not rare. In the same way, among the leadership of an organisation, too optimistic or indifferent views on information security risks and threats as well as one own vulnerability or exposition, frequently come up. Consequently, information security, in many cases, is understood as an unnecessary cost and as a function demanding too many means (Igor Bernik & Prisljan, 2016). To overcome the wrong convictions, an understanding of the implications of risks and actual input from information security to commercial or organisational success must be provided for on the leadership levels.

The relevance of information security for organisations may be seen similarly to the commercial value of ICT and information systems. Commercial value of ICT is provided for when it contributes to a higher effectiveness of commerce and a higher competitiveness of an organisation (Melville, Kraemer, & Gurbaxani, 2004). Departing from such a view, the added value of information security is reached when expected positive effects and influence on the conduction of commercial processes are reached.

With a proper approach to management, information security may have numerous short-term and immediate, as well as long-term and mediate effects. *Immediate or operative effects* are visible in a more effective conduction of processes and commerce, as through the definition of accountability, reduction of incidents and better reaction to events, a contribution to lower interruptions, quicker reactions, a higher situational awareness, better surveillance and consequently lower costs connected to security incidents is made. Mid-term and long-term effects give *tactical and strategic advantages* to organisations. Effects of a strong and qualitative information security are seen in improved relations with partners, a higher compliance, positive external audits, a higher level of trust or legitimacy and reputation in the public (Enzineard et al., 2005; Wlosinski, 2019). A high integrity, trust and a positive public image belong among the main long-term effects of information security. Implications of this kind may contribute to a higher market value of the enterprise and commercial advantages on the market. Namely, showing a high responsibility in providing for information security frequently is a pre-condition for entrance into commercial connections, partnerships and acquisition of new business, mainly in the international context (BSI, 2018; Enzineard, McFadzean, & Birchall, 2005).

In the opposite case, when organisations do not invest in information security development and management, the implications of the success and reputation of organisations may be extraordinarily negative. The consequences of realised information security incidents may be divided into financial or immediate and mediate or long-term consequences. *Financial consequences* most frequently show in the form of damage appearing from cancellations and interruptions of work processes or in a lower sale of services and products. Besides, among immediate costs also belong financial sources needed for recovery and healing from the consequences. One must respect that abuse or loss of personal data or data on foreign property leads to civil legal claims or criminal accusations. Besides financial consequences, information security incidents may also have *other negative effects* that are harder to measure but may have even worse consequences. They influence immaterial assets and refer e.g., to loss or decrease of reputation in the commercial environment and on the market. In case of a bad information incident, an organisation may become a target of attention from the media, influencing the opinion and convictions of clients and/or business partners and may contribute to a loss or decrease of commerce. Potentially, public accusations and decrease of credibility may follow. At the same time, also the competitive advantage may be

endangered, when intellectual property and business secrets are stolen or alienated (Agrafiotis, Nurse, Goldsmith, Creese, & Upton, 2018; I. Bernik, 2014; EDUCAUSE, 2019a; Prislán & Bernik, 2019; Tayaksi, Ada, Kazancoglu, & Sagnak, 2021).

Besides all mentioned advantages and positive effects of information security on the commercial success of an organisation, mainly its contribution to business continuity and compliance is of key importance.

Business continuity generally refers to the capability of an organisation to maintain and tackle unpredicted events successfully. This means that the organisation can survive unpleasant situations – it is able to do business or resurrect its processes and continue business in spite of catastrophes, incidents or environmental influences. A composite part of this is the preservation of functioning and renewal of key business processes. Business continuity is a part of strategic management and, in modern organisations, includes reactive (plans and processes for recovery) as well as proactive (plans and processes for resilience) functioning. There, information security is merely one of the fields contributing to providing for business continuity, as unpredicted events may be connected to most various risks, and it is a fact that threats and incidents in connection to technological development and progress of an organisation strongly threaten the capacity of business continuity (Niemimaa, Järveläinen, Heikkilä, & Heikkilä, 2019).

Compliance is one of the pre-conditions to be met by an organisation, as by this, they meet the demands for legal and legitimate business. Providing for compliance is connected to various fields, and it is especially relevant in the context of information security, where prescribed demands regarding privacy, personal data protection and information system security must be met. Within information security, in the first place, it refers to respect for legal regulations and the conduction of measures within their framework. Information security must be regulated in a way prescribed by legislation – in the management, processing and protection of data and information systems, prescribed measures are taken, and at the same time, no exaggerated or disproportional control is carried out. This means that the rights of those who are object to security measures, e.g., the data and system users, are respected. Organisations must know all key legal acts referring to their business and security and must take care of meeting these demands by proper measures. Disregarding the

kind and structure of an organisation, meeting legal provisions is obligatory, else prescribed accountability is violated, and legal consequences might follow. Besides a legal compliance, there are also other aspects of compliance referring to respect and following of internal acts, contractual obligations and other professional and international directives or good practices. Thus, compliance as field of information security implies the following aspects: compliance with (national and international) legislation; compliance with the organisational strategy and internal rules and instructions; compliance with obligations departing from contracts, and agreements; compliance with standards and recommendations in the field of information security; and compliance with (national, international) strategies (Prislán & Bernik, 2019).

4 Approach to providing form Information Security

To increase of complexity of information systems and information security risks in organisational environments, among experts, a position has been established that information security must develop as a business function and special organisational activity (Baskerville, Spagnoletti, & Kim, 2014; Bojanc & Jerman-Blažič, 2008; Chang & Ho, 2006; Feng, Wang, & Li, 2014; Mishra & Chasalow, 2011; Thomson & von Solms, 2006), and in management an interdisciplinary and team approach is necessary. Everybody responsible and competent to provide for information security in an organisational environment must be aware that information security is not just a matter of a purchased technical product or exclusive responsibility of the IT department, but a matter of the whole organisation, as the leader as well as each employee, as it is them, who take care that the definitions of rules become alive in practice (Prislán & Bernik, 2019).

Accountability for providing information security lies in the hands of three groups inside an organisation, as there are: *owners* of information sources (are owners of information and accountable for the definition of their confidentiality); *custodians* of information sources (are defined by the owners and accountable for operative conduction of measures and rules of information security, surveillance of the state and reporting to owners); *users* (the use information sources at work and are accountable for respecting the information security rules and policies) (Whitman & Mattord, 2012). Concretely, basic accountability is divided between the top and the operative management, among the main work spaces having determining functions

or being connected to information security management, belong: CEO (*Chief Executive Officer*), CIO (*Chief Information Officer*), SAISO or CISO (*Senior Agency Information Security Officer* or *Chief Information Security Officer*), AO (*Authorizing Official*), SAOP (*Senior Agency Official for Privacy*), SSO (*System Security Officer*), ISA (*Information Security Architect*), SSE (*System Security Engineer*), SCA (*Security Control Assessor*) and SA (*System Administrator*). Among support personnel cooperating in the management process belong the responsible staff for fields as there are: physical security, audit, quality, personnel, crisis management, privacy, and similar. There, such detailed division of staff usually is characteristic for larger organisations, whereas in smaller organisations, they usually might be united (Nieles et al., 2017). In discussions on the way of organising and placing information security functions (and personnel) in a hierarchic structure, the importance of providing for a direct communication/report line of accountable staff towards the leadership level and the best possible (financial, decision-making, personnel) independence of this function is stressed (Goodyear, Portillo, Goerdel, & Williams, 2010; Klimoski, 2016).

In line with the complex nature of information security in organisations, it is frequently compared to a puzzle – it is composed of multiple parts that must be compliant and connected. Here, the authors define different fields and dimensions of information security; some of them are presented below.

De Oliveira Albuquerque, Villalba, Orozco, Buiati, & Kim (2014) describe the TISA (*Trust Information Security Architecture*) model, where four fields of information security and measures connected to it are defined. The *first field* encompasses planning of measures and includes activities in connection to the identification and assessment of confidentiality of information systems and information sources, providing for their integrity, confidentiality and availability, management of digital identities, access control, cryptographic data protection, and protection of privacy and anonymity. The *second field* encompasses the definition of rules, which includes adopting an information security policy. The *third field* includes the conduction of operational activities and mainly refers to the surveillance of processes and respect for rules, the performance of audits and supervision of information security risks. The last and *fourth field* intervening with the other three refers to trust-building, where it is about strengthening legitimacy, compliance and verification of integrity with the purpose of building a system, where expectations as well as goals are met.

Von Solms (2001) as an example mentions 12 different dimensions that together form a system of information security: the *strategic dimension* includes activities connected to planning and support; the *organisational dimension* includes processes connected to management; the *political dimension* includes activities connected to definition of information security strategy and policies; the *ethical dimension* refers to transparent decision-making and conduction of measures; the *certification dimension* refers to processes of accreditation; the *legislative dimension* refers to providing for compliance; the *insurance dimension* encompasses insurance for cases of information incidents; the *personnel dimension* refers to processes and measures connected to users; the *cultural dimension* includes development of a security culture; the *technical dimension* refers to planning and conduction of technical measures; the *evaluation and audit dimension* includes processes connected to assessment of effectiveness, audits and controlling.

Similar descriptions come from Hagen, Albrechtsen, & Hovden (2008), who connect effective information security to four intertwined fields: the *management perspective* refers to processes of information security risk management; the *economic perspective* includes demands for economic and rational investments; the *normative perspective* includes providing for compliance, the *cultural perspective* refers to the development of security culture and awareness.

According to the variety of fields forming an information security system and heterogenous factors influencing the state of information security, decisions of management must be based on an analytical or systematic process. In this process, organisations must manage and master information security risks: this means that they must periodically analyse the actual state of security and risks and, based on the cognitions, take decisions on proper ways to provide information security. Such an approach is comprised of an information security system described in detail below.

4.1 ISMS and Information Security Risk Analysis

ISMS (*Information Security Management System*) is an array of measures, procedures and policies for systematic data security management in an organisation. The goal of such a system is pro-active addressing of information security risks and decrease of effects by eventual incidents.

The model or framework of ISMS is defined in the international standard ISO/IEC 27001. The latter describes a model of composition, maintenance or preservation, surveillance, and improvement of ISMS, while directives and controls for meeting the pre-conditions and demands from ISO/IEC 27001 are presented more detailed in the standard ISO/IEC 27002. The mentioned standards are a part of the family or series of standards ISO 27000, addressing various aspects of information security management.

The range and contents of ISMS must respect organisational specifics, and therefore standards for building the system are relatively flexible and adaptable (in case that the organisation wishes to be certified according to the standard, certain demands and pre-conditions are obligatory to be met, others are optional). Building and introduction of ISMS in a certain organisation is influenced by its goals, vision, security requests, processes, size, and organisational structure. The influence and running of ISMS are mostly influenced by security requests depending on the nature of the commercial branch, form of business and commercial processes, technologies, connected subjects (partners, suppliers, and similar) and information security risks faced by the organisation.

The building and maintenance process of ISMS is based on the PDCA (*Plan, Do, Check, Act*) model. From this point of view, ISMS is a circular process that must be constantly assessed, supervised and updated after planning and building, what means that the process really does never end. Below (table 1) activities within each individual phase of building ISMS in line with the steps defined in the PDCA model are described in more detail.

Presented levels of ISMS and individual activities represent a systematic approach to information security regulation. Regarding the needs, an organisation may widen individual phases (e. g., the establishment of compliance may be a separate process/project), and opposite to this, individual phases may be joined. Due to the flexibility of the model, organisations may introduce ISMS into their own structure in different ways.

Table 1: Building ISMS in line with PDCA model

Phase	Activities
<p><i>Plan.</i></p> <p>Start of ISMS</p>	<ul style="list-style-type: none"> - Decision on introduction and way of introduction - Definition of range and limits of ISMS - Definition of approach to risk assessment - List of information - Status analysis - Validation and risk assessment - Analysis of possibilities of risk handling - Selection of control - Plan of handling - Obtaining approval from leadership - Assessment of compliance with legislation
<p><i>Do.</i></p> <p>Introduction and Performance of ISMS</p>	<ul style="list-style-type: none"> - Implementation of plan for risk handling - Implementation of control - Definition of methodology for assessment of effectivity - Implementation of training and education programmes - Means management - Implementation of measures for incident recognition
<p><i>Check.</i></p> <p>Surveillance and control of ISMS</p>	<ul style="list-style-type: none"> - Surveillance and control, failure discovery - Regular analysis of effectiveness of control, measures and processes - Risk control and surveillance - Leadership controls - Addition to plan, policies, ISMS documentation - Notification of events that may influence security and effectiveness
<p><i>Act.</i></p> <p>Maintenance and Improvement of ISMS</p>	<ul style="list-style-type: none"> - Correctional and preventive measures based on established lacks in the past step - Reporting - Follow-up on corrections

Information (Security) Risk Management is a composite and key part of providing information security. It is about a process, where it is established, what risks threaten an organisation, what are more or less frequent/dangerous and how to prepare for them. After the definition, an *information security risk represents a probability that an unpleasant event or incident will happen*. As mentioned, it is not a goal to provide for total security, and therefore in the process of risk analysis, it must be established, what risks are most dangerous and probable. For the calculation of risk or probability, a threat assessment, an assessment of vulnerability and an assessment of consequences are needed. Thus, *information security risk analysis* is a composite part of the information risk management process that is a process of assessing the organisational state in a quantitative form. Like the building of ISMS, also in information security risk

management, it is important to conduct the process constantly (periodically) and systematically throughout individual phases and steps that might be joined or widened for practicality and rationality. Thus, in the process of information security risk analysis, the needs of organisations are established, and responses to relevant questions are received (*ISO/IEC 27005:2018*), as there are: *why we need protection, what are we going to protect against whom or what are we going to protect ourselves and how are we going to regulate protection.*

Basically, the process of information security risk analysis is divided into three main phases (ENISA, 2015; Whitman & Mattord, 2012):

1. *Identification:*

- Identification (listing), classification, and prioritisation of information and information sources
- Identification, prioritisation, and assessment of information threats
- Identification of information vulnerability

2. *Assessment:*

- Determination of methodology
- Risk calculation

3. *Control:*

- Determination of acceptable risks
- Selection of strategy for handling risks
- Assessment of benefits and feasibility of the strategy
- Argumentation for the decision and reporting to interest groups
- Implementation, control or surveillance and maintenance of measures.

When selecting the approach, the organisation defines the range of the analysis and builds a plan; then it conducts the analysis of all major elements, makes the calculation and takes a decision on how to handle the risks. Here, various possible decisions are at hand, as there are: *acceptance of risks* – no reaction; a *decrease of risks* –

reactive measures; *mastering risks* – preventive measures; *avoiding risks* – getting rid of or dropping of elements creating vulnerability; *risk transfer* – transfer of accountability to a third subject. If the organisation decides to take measures, various security measures are at hand for this purpose.

Through similar steps, the risk management process is also defined by the standard *ISO/IEC 27005: 2018*. Regarding the directives by the standard, the mentioned process runs through five phases: (a) determination of a reference framework for analysis; (b) risk assessment; (c) decision-making regarding risk handling; (d) notification of interest groups; and (e) follow-up, surveillance, verification and updating of measures.

For easier planning and conducting of the described process, besides orientations contained in different standards and directives (e. g. *ISO/IEC 27005*, *BSI 100-3*), organisations also have more practical models at hand, as well, e. g. *OCTAVE*, *MEHARI* or *MAGERIT* models (Hommel et al., 2015).

4.2 Information Security Risks, Threats, Vulnerabilities and Measures

Situations threatening the state of information security differ by intensiveness and degree. Generally, potentially dangerous situations categorise as a security event (phenomenon representing a deviation from the normal state or having a potential threat to information security) or security incident (an event likely to threaten business and data security) (*ISO/IEC 27000: 2018*, 2018), and the way of response and measures depends on the classification,

An information event is a deviating phenomenon in the use of data or an information system representing some unpleasant situation of state of potential danger, but not necessarily leading to damage. An *information incident* is a real danger for the organisation and the state, where measures must be taken (Nieles et al., 2017). Organisations must be well-prepared for incidents, and they have to place attention also on other events, as by false handling, they might grow into an information incident. Events and incidents realise when a vulnerability used by the threats is present in the security system.

Thus, information security risks lead to unpleasant phenomena influencing or threatening the state confidentiality, integrity or availability of information systems and data. Key elements of information security risks are *information sources, information threats, information vulnerabilities and information security measures (ISO/IEC 15408-1:2009)*. When vulnerabilities appear on a certain information source level, there is a potential danger that an (intentional or unintentional) threat using vulnerability with a certain technique might become a reality. Whether the threat will become a reality and lead to an incident or not is depending on the measures protecting the sources or decreasing vulnerabilities.

Information sources are data and information capital owned (or managed and processed) by an organisation. Among the most relevant data managed by organisations belong personal data, financial data, secret data, business secrets, intellectual property, data of business partners or connected subjects, passwords and data in connection to digital identities as well as services of trust and other data relevant for development and competitiveness of an organisation (e. g., strategic and development plans). Data must be protected and secured in all phases of management (establishment, processing, saving and transfer), disregarding their (digital or physical) form. As data are managed with the help of information systems, among relevant elements to which threats and vulnerabilities are connected belong also to other components of organisational information systems (technologies (software, hardware, networks, mobile tools, etc.), people and processes). Here, actual reports (Verizon, 2021) show that among the most targeted data of cyberattacks belong passwords, usernames, personal data, health and bank data.

Information threats are situations or phenomena that may use vulnerability on the level of information systems and, by this threaten confidentiality, integrity or availability of data and lead to an information event or incident. Information threats may be intentional or vicious, or unintentional. The first group is most frequently connected to planned vicious actions by (external and internal) individuals, organisations or other groups who want to use or harm an organisation. In this case, it is about the so-called cybercrime.² Among these, mainly financial and also espionage motives

² An international definition of forms of cybercrime was given by the Council of Europe in the (*Convention on Cybercrime, 2001*)², where five kinds of criminal acts were defined:

- crimes against confidentiality, integrity and availability of computer data and systems (illegal access, interception, disturbance and abuse of data, systems and installations),

prevail (Verizon, 2021). Unintentional threats include natural and other disasters, unplanned failures and errors in user data and systems. The American National Institute for Standards and Technology – NIST (Nieves et al., 2017) sorts vicious threats to information security in fraud and data theft; malware, hacker attacks, cyberespionage and insider threats; and unintentional in failures and errors at work, loss of equipment and documents and loss of privacy in sharing information publicly.

European Network and Information Safety Agency (ENISA, 2020a) sorts the most widespread contemporary cyberthreats in infection with various sorts of malware, web-based attacks, fraud or phishing, web application attacks, spreading of spam mails, denial of service, identity theft, insider threats, physical manipulation, damage, theft and loss as well as cyberespionage. Here, it is important to mention that social networks are increasingly used for attacks and data collection, and hacker attacks, attacks with social engineering and infections with malware, where *ransomware* represents a huge problem, are among the most problematic threats for organisations from the described (ENISA, 2020; Verizon, 2021).

Despite the prevailing external threats or external attacks on the information systems of organisations, a special challenge is represented by information threats coming from the insider environment, as it is harder to discover them in comparison with external threats (ENISA, 2018; Verizon, 2019). In case of the so-called *insider threat* that might be described as a situation when a person or a group connected to the victim (with access to the victim's information systems, networks and/or data) exceeds or abuses these access rights in a way that it has negative consequences for information security – i. e. creates risks for confidentiality, integrity or availability of information or information systems (ENISA, 2020b; CISA, n. d.). Insiders are persons with legitimate rights to access confidential or sensitive data and may be

-
- computer-related crimes (computer falsification and fraud),
 - content-related crimes (children pornography),
 - copyright crimes and crimes related to similar rights,
 - racist and xenophobic actions and expressions of inappropriate statements towards genocide or crimes against humanity committed in computer systems (this group of actions is defined by the additional protocol to the Convention on cybercrime).

The convention prescribes that the signatory states take care for incrimination of the mentioned forms of crimes in their legal orders, take care of capability and capacity of immediate insurance of computer and traffic data, search of computer installations, interception of data and traffic as well as real-time insurance of data. The importance of international cooperation and support in investigations of cybercrime is stressed.

aware of the vulnerability of an information system (they may be employed, be ex-employees, contractors, business partners or collaborators) (Homoliak, Toffalini, Guarnizo, Elovici, & Ochoa, 2019; Jordan, Hawron, Jordan, & Hawron, 2015; S. L. Pfleeger & Stolfo, 2009; The CERT Insider Threat Center, 2016; Warkentin & Willison, 2009). The main reasons why violations and failures of employees or users appear may be comprised of five groups, as there are: lack of motivation to respect security rules; lack of knowledge of risks and attacks; inappropriate or risky convictions; inappropriate or risky behaviour; inappropriate use of technology (Badie & Lashkari, 2012). The worst abuses may happen mainly by privileged users, as they have knowledge of processes and systems in organisations, access to critical parts of a system and configurations of security mechanisms. Besides vicious (former or present) employees, who want to take revenge or damage an organisation for various reasons, a large problem is also unaware or careless employees or users, who enable an attack by external criminals by their negligence. Unaware and negligent users/employees may harm an organisation because of a disclosure of confidential information by error, reactions to phishing emails and malware, visits to inappropriate websites, thoughtless upload of contents, connecting equipment, enabling unauthorised access to data or information systems or because of losing or alienating electronic equipment and documentation (ENISA, 2017, 2018). Reports show that actually more than 80 % of all cyberattacks on organisations are connected to a human element, and among those where employees are the main cause, abuse of user rights and inappropriate handling of data prevail (Verizon, 2021).

Information vulnerability is defined as a security gap or weakness, error or deficiency in an information system (on the level of sources, processes or protection) (ISO/IEC 27000: 2018, 2018; Nieves et al., 2017) that alone does not cause negative consequences, yet. Negative consequences come up if vulnerability is used by information threats. Information vulnerability increases together with complexity and range of an information system. As information systems are composed of different elements, information vulnerability appears in different forms. Among the most targeted elements of information systems are servers, mobile equipment and laptops, as well as people or users (Verizon, 2021).

With the COVID-19 pandemic that caused drastic transformations in work processes and introduced home office or distant work in a majority of sectors, new challenges and risks connected to distant access, use of cloud technology, data transfer into private environments, sharing of files, video conference meetings and similar started to show up. During this time, criminals developed more personalised and sophisticated forms of user rights theft, phishing, social engineering, spreading of malware and attacks on mobile telephone platforms (ENISA, 2020). Among the main vulnerabilities connected to insider threats belongs e. g. inappropriate management of privileged rights, an increase of the amount of confidential data and an increase of the amount of equipment with access to confidential data, use of mobile equipment at the workspace, the high complexity of new technologies for users and the low degree of awareness among users (ENISA, 2017).

Besides the described elements, information security risks were finally strongly influenced by *security measures* (or security controls and mechanisms). Security measures are methods, rules or proceedings of organisations to oppose threats or correct vulnerabilities and to prevent or lower risks in this way.

In providing for information security situational surveillance measures (related to the use of mechanical, technical or software control) or managerial or organisational measures (activities related to addressing behavioural, procedural, political, environmental and normative aspects) may be taken. In line with this, international directives and normative acts, as a rule, divide information security measures into organisational (e. g., definition and formation of processes, accountability, education and training and raising of awareness), legal (e. g. providing for compliance, acceptance of policies, strategies, standing orders and agreements), logistical and technical (e. g. software control on the level of computers and user equipment, servers and databases, networks controlling and limiting access of traffic) and physical (e. g. physical obstacles, access control and protection from disasters) ones.

Measures of providing for information security may be divided into internal and external as well as preventive and reactive ones. External measures are mechanisms by which threats coming from the external environment of an organisation are mastered, and internal measures address threats coming from the internal environment. Preventive measures try to prevent the realisation of (situational or social) information incidents, while reactive measures are reaction mechanisms to

prepare an organisation for eventual incidents with the aim of an effective reaction, limitation of damage and healing (Allen & Westby, 2007; Kankanhalli, Teo, Tan, & Wei, 2003; Sethuraman & Adaikkappan, 2009). Measures may be more concretely divided further into measures of rejection (decrease of attractiveness or accessibility of a target), prevention (limitation and control of use of information systems); recognition (detection systems); and healing (normalisation of state after an incident) (Pfleeger & Pfleger, 2006).

The international expert organisation Center for Internet Security – CIS (2020) formed a list of 18 measures (*Critical Security Controls*) for cyberdefence that have been recognised as the most effective ways to stop contemporary threats and attacks. The list presented below represents a collection of high-priority measures formed in line with the *Parett* principle 80-20 that follows the idea that by executing a smaller collection of key activities, a major share of problems and vulnerability can be abandoned. The list, in line with international information security standards, has been developed since 2008 and is constantly updated regarding changes in technology development and threats. Measures are defined based on an analysis of the most frequent patterns of cyberattacks through sharing of knowledge and mutual adaptation and development by a vast consortium of governmental and industrial experts from different profiles.

- 1) Inventory or list of property and equipment of an organisation.
- 2) Inventory or list of software (definition of allowed and identification of unallowed software).
- 3) Data security (list and categorisation of data, security through the whole lifecycle).
- 4) Security configurations of the property and software of an organisation (e. g. possibility of remote control over equipment in case of theft or loss, configuration of firewalls, servers).
- 5) User account management (e. g., deletion of inactive, useless accounts, protection from hacker intrusion, attacks with raw force).
- 6) Access control management (e. g. multiple factor authentication, minimum privilege policy).
- 7) Continuous vulnerability management (e. g. regular updating of systems and implementation of security upgrades).
- 8) Surveillance of daily protocols.

- 9) E-mail and search engine security (e. g. antivirus protection, protection from unwanted e-mails, limitation of access to the homepage).
- 10) Protection from malware.
- 11) Data renewal capacity.
- 12) Network infrastructure management (e. g. updating and configuration of firewalls, routers, servers, administrator account safety).
- 13) Network supervision and safety (e. g. SOC, SIEM, IDS, IPS, VPN or centralised management, network segmentation, remote access security).
- 14) Raising awareness and training of users.
- 15) Management of connected subjects (partners, suppliers with emphasis on suppliers of cloud services).
- 16) Application security (e. g. security tests and application check-ups).
- 17) Incident reaction management (e. g. regular testing of plans).
- 18) Penetration tests.

In the phase of planning measures, it is important to have in mind that internal factors are those that most frequently enable the realisation of external threats. By focusing exclusively on technical aspects of security, an organisation might be protected from some external attacks and threats, but it still remains vulnerable to the most dangerous threats (Spears & Barki, 2010). Besides awareness programmes and user motivation, for the prevention of internal threats, an access and user rights management is of main importance. Only by preventive rules the possibility of abuse can be limited in a way that users obtain a range of use to the extent of obligatory necessity and exclusively to data connected to the content of their work (Bunker, 2012). From the point of view of surveillance, besides strong authentication processes in an organisation, so-called UBA (*User Behaviour Analytics*) solutions and procedures enabling surveillance of usage of a system and detection of anomalies or potential data abuse come to use more and more.

At individual scopes or groups of listed measures, various security solutions offered by different suppliers are at hand, but in the planning of measures, it is also necessary to have in mind rationality and functionality, as well as protection of the right to privacy. As already mentioned, namely, controls might be successful and provide for a high degree of security, but at the same time also irrational and ineffective (e. g. when too many measures are used or measures that are too limiting or invasive in relation to the level of risk). Hagen et al. (2008) say that information security

measures are effective when four pre-conditions are met: (a) when risks are at minimum level; (b) when investment in measures is rational and meaningful; (c) when measures are in line with provisions and legislation and (d) when users understand and really respect the measures.

4.3 Standards and Recommendations

When planning formation of ISMS and information security management, organisations dispose of support by different international standards. In Attachment A, some most well-reputed international standards and directives regulating field connected to information security management shall be comprised.

Following actual trends in the field of information security and cyberthreats, besides the mentioned standards, organisations may get support also by research and reports of various security enterprises and expert associations. Besides annual reports published by national response centres - CERT, among such reports published annually or periodically, are following:

- Cost of cybercrime study (Accenture and Ponemon).
- Data breach investigation report (Verizon).
- Global corporate IT security risk survey (Kaspersky).
- Global information security survey (Ernst & Young)
- Cybersurvey (Deloitte).
- Global state of information security survey (PWC).
- Cybersecurity breaches survey (Department for Digital, Culture, Media & Sport).
- Information security threat report (Symantec).
- Norton cybersafety insights report (Norton).
- Global cyber risk perception survey (Mesh and Microsoft).
- Threat landscape (ENISA).

5 Information Security and Higher Education Institutions

From the aspect of cyber and information threats, academic and research institutions belong among the most exposed organisations, as they manage numerous sensitive financial, academic and administrative data, mainly saved in electronic or digital form and by this, vulnerable to numerous attacks and abuses (Aguilar Quintero, Velásquez Pérez, & Castro Silva, 2019). In recent years, higher education institutions, with growing connectivity, face a huge increase in information security incidents, and therefore demands for a stronger personal data security and privacy are stepping into the foreground (EDUCAUSE, 2021; Ulven & Wangen, 2021). Since the needs for information security already exceed the capacities and accountability of individual technical staff or smaller departments in education institutions, a trend of frequent implementation of demands by international standards and establishment of specific workplaces like CISO and authorised personnel for personal data security can be seen in the past decade (Hommel et al., 2015).

Compared with other organisations, education institutions function under specific circumstances, strongly influencing needs in connection to information and cybersecurity. Vulnerability is high already due to the nature of the higher education branch that is based on academic freedom, openness, accessibility and transparency (including information systems and data), as well as due to the high level of digitalisation and connectivity (Campbell, n.d.; Hina & Dominic, 2017; Ulven & Wangen, 2021). Information systems and information technologies represent a critical and fundamental part of processes running in the higher education branch, and technological innovations represent the ground of its development and growth, while also vulnerabilities connected to data security and privacy of users increase (EDUCAUSE, 2021). From the aspect of processes, the culture of trust, connecting, cooperation and teamwork create an environment open for sharing and exchanging data (Adams & Blanford, 2003).

Among the special characteristics of education institutions, due to which they differ from other branches and that are important for information security, there also belong (Campbell, n.d.; Dell, 2018; EDUCAUSE, 2021; Fishman, Rudnicki, & Grama, 2021; Hommel et al., 2015; Ulven & Wangen, 2021; Vrhovec & Mihelič, 2021):

- Universities and departments manage enormous amounts of sensitive and confidential data (personal and financial data of employees, students, intellectual property, sensitive and confidential research data, data on partner organisations, etc.) because of what incidents in connection with abuse, theft or disclosure of these data lead to unimaginable consequences for the reputation of a university, as well as the safety of employees and students. Generally, a high degree of fluctuation of staff, students and visitors are characteristic for higher education institutions. Namely, on a daily level, there are many people or individuals who enter buildings and spaces of an institution as well as information systems.
- Interconnection of office and private life being traditional in an education and research institution is connected to the increasing use of private ICT for office purposes (*Bring Your Own Device* - BYOD). In education environments, the use of various portable or mobile equipment that connects to networks of the organisation is extraordinarily frequent, and in the same way, private and office data get joined on users' or staff's equipment. Mobile equipment represents an extra high vulnerability or risk, as students, visitors, as well as employees connect with their various mobile and smart equipment to networks, access data and applications.
- Servers managed by higher education institutions and accessible via the internet represent an attractive target to criminals. Namely, besides data, infrastructural sources, such as high-performance processors, networks and servers are interesting to them, as by the manipulation of these, sophisticated DDoS attacks can be performed, or malware or spam can be distributed.
- Increasing distance education increases the use of open internet learning environments, videoconferencing tools and data sharing via the internet. Today, pedagogical processes and students prevalingly work in a digital environment, many processes and functions are conducted through the internet. Even connections between different education institutions and researchers are increasingly intensive and frequent, which results in an implementation and use of complex tools and environments for collaboration. In times of pandemic, vulnerabilities in connection to the use of new technologies have increased, since there was a total move of pedagogical and research activities into cyberspace.

- Vulnerabilities are also represented by advanced technologies that are being introduced to support innovative forms of education and training, as there are virtual and augmented reality (VR and AR). The use of such technologies is frequent for the needs of simulation (e.g., in fields of natural sciences and technologies) and realistic collaborations. These systems frequently are weakly protected and vulnerable to intrusion and abuse (e.g., do not use coded network connections; users use personal equipment bypassing established protocols for authentication; offenders create a twin profile or avatar or use vulnerability of sensors, cameras and microphones). Attackers may abuse mentioned vulnerabilities to gain access to tools and applications for cooperation and destruction, data, communication or infection of an organisation's network.
- For the education branch, fragmentation of networks and mutual connectivity of these networks is characteristic, as well as a vast inter-organisational environment creating a wide network of connected systems and data. Further, the use of services and data saving in clouds becomes more frequent, creating new or larger vulnerabilities and possibilities of abuse.

To sum up, higher education institutions have a great challenge represented by their need to a parallel balancing of demands for security, resilience, and surveillance on the one side and needs for openness, accessibility connectivity, privacy, innovation and flexibility on the other side.

5.1 Information Security Risks in Higher Education

One of the most important information properties managed by education and research institutions that can be subject to abuse are data on students, financial data, research data and data on employees. In addition to these data that belong to the most sensitive data, also other data are relevant for information security, e. g., study materials, learning plans, exams, and leadership and management data (Ulven & Wangen, 2021). Mainly research cognitions and achievements belong to the most targeted data and information (EDUCAUSE, 2021; ENISA, 2020), as well as personal data and user names and passwords (Verizon, 2021).

Among the most frequent cyberthreats endangering the education branch, ENISA (2020) ranks malware, ransomware, internet attacks, and in the past year, even an increase of cyberespionage was noted. As a consequence of a vast amount of data managed by education institutions, in such a branch, one can notice a trend of increased targeted attacks (Hommel et al., 2015). For higher education institutions, attacks with social engineering are a huge problem since more than a third of data abuse is connected to such a threat (Impact, 2021). A study on susceptibility and vulnerability by phishing attacks between different branches and industries showed that the education branch ranks in fourth place (thus among the most vulnerable branches), with a success rate of phishing fraud of 13 % (Proofpoint, 2021). In its annual report, also Verizon (2021) lists social engineering attacks among relevant threats to higher education institutions in the same way also (D)DoS attacks that represented more than half of the attacks on the education branch in 2019. From the aspect of malware, ransomware represents the largest threat and the majority of infections in higher education institutions. In addition to the mentioned, a frequent cause of incidents are also attacks by employees e. g., by intentional disclosure of data or wrong use of systems as well as violations of policies, loss or theft of electronic equipment (Ulven & Wangen, 2021).

Among criminals targeting the education branch, financially motivated and highly capable hackers prevail. With sophisticated techniques and methods, they aim at obtaining and selling personal or confidential data or want to use capacities or capabilities of the technologies managed by higher education institutions in order to conduct other attacks. Besides financially motivated hackers, activists and those, who act for the purpose of state-supported espionage, represent a frequent group of criminals, as well. Incidents are also connected to the criminals, who want to cause intentional damage or breakdown of information systems or test security protocols, not rarely also disappointed students or (ex) employees, who want to take revenge, appear among the criminals (Dell, 2018; Ulven & Wangen, 2021; Verizon, 2021).

A study from 2020 among 500 employees from higher education branches showed that more than a third of education institutions had witnessed a cyber attack in the past, and one-fifth had witnessed such an attack during the time of pandemic (Morphisec, 2020). A study conducted among higher education institutions in Great Britain showed very similar results since in the period from 2015 to 2020, 33 % of the education institutions went through an attack with ransomware (TopLine

Comms, 2020). In the past two years (2019-2021) or during the time of the global COVID-19 pandemic, respectively, in higher education institutions, numerous critical and medical exposed information security incidents were realised. Below, some most well-known are exposed:

- Australian National University: a hacker attack caused data abuse of 200.000 people.
- University of Greenwich: compromising of sensitive data of 19.500 students resulted in a fine of 160.000 dollars.
- Washington State University: an infection with malware led to abuse of personal data of 4.5 million people.
- University of Connecticut: a hacker attack led to compromising of personal data of 326.000 people.
- Monroe College: an infection with ransomware led to a payment of 2 million dollars in ransom.
- University of California: an infection with ransomware led to a payment of 1.14 million dollars in ransom.
- German University Hospital Düsseldorf: an infection with ransomware resulted in a victim of death.
- Harrison Federation: an infection with ransomware disabled 37.000 pupils of elementary schools in Great Britain from accessing e-mail.

Besides the mentioned, other universities were victims of ransomware, as well (e. g., Oregon State University, Michigan State University, Kent State University, University of Dayton, Columbia College University, and in the USA, even several elementary and secondary schools (*K-12 Schools*) were victims of such attacks (Morphisec, 2020).

Vulnerabilities appearing in the higher education branch and representing an opportunity for criminals and increase risks are of organisational as well as of technological nature. From the technical point of view, in higher education institutions inadequate e-mail security frequently represents a problem, as well as processes of user rights management (Verizon, 2021). Undeveloped or weakly developed detection and reaction capacities, inadequate authentication processes and information system access management also represent an important challenge

(EDUCAUSE, 2021). Because of the culture of openness, frequently also strong physical controls connected to entry and exit are absent or rare (FireEye, 2014). Ulven & Wangen (2021) list inadequate management of mobile equipment; inadequate data protection protocols through processes of data obtaining, creation, saving, processing and transfer; absence of technical key measures defined as good practice and vulnerabilities connected to complexity and splitting of networks among the main technical vulnerabilities of higher education institutions.

Employees belong to important vulnerabilities of education institutions, as well, as almost half of the incidents are connected to employees and their failures at work (Verizon, 2021). From this aspect, mainly a lack of awareness and training management for staff and students is representing a problem and in addition to that also an inadequately developed security management and information security management approach, a lack of leadership support and an improper attitude towards information security as such (Ulven & Wangen, 2021). According to this, mainly a lack of a holistic approach to system security management that is supposed to upgrade technical measures and to include activities directed to the development of a strong security culture among employees and students is stressed to be an important challenge (Hina & Dominic, 2017).

It also must be mentioned that higher education institutions were among the first branches that followed the trends of digitalisation, and this is why the first-aged systems are still in use and they are highly vulnerable. Due to decentralisation, autonomy and high variability among individual departments or institutes, ICT management and security is also frequently decentralised, which hinders transparency, unified management and quick response. Like in other branches, higher education faces a lack of specialised personnel in the field of information and cybersecurity. (Campbell, n.d.; EDUCAUSE, 2019b, 2021; FireEye, 2014). In 2018, more than half of higher education institutions (n = 3,800) still did not possess regularly employed staff for the field of information security. Also, a lack of financial resources represents a problem and disables the use of contemporary security solutions. Namely, higher education institutions prevalently are publicly financed and cannot afford higher financial investments enabling the purchase of more updated solutions. An overview of state-of-the-art from 2018 also showed that higher education institutions dedicated only 3,6% of the total IT budget for IT security (EDUCAUSE, 2019b). Consequently, higher education institutions

frequently are capable only of reactive functioning (response to incidents), but proactive security from more contemporary threats is not developed (Dell, 2018; Fishman et al., 2021).

For providing for an adequate level of information security and in this context for privacy and personal data security, as well, the most important measures that should be taken by higher education institutions are (Buzzelli, 2021; Campbell, n.d.; Ulven & Wangen, 2021):

- access control mechanisms, which include a multi-layer authentication, a minimum privilege policy as well as physical security of location and equipment from abuses, damages, theft, accidents, etc.
- identification and prioritisation of critical systems and data management throughout the whole lifecycle (protocols connected to digitalisation, transfer, sharing of data, archiving, destruction, access or collection).
- maintenance of audit trails, and verification of integrity.
- safety copies, regular updates and security reparations.
- internet attack security, mainly security from SQL and phishing attacks, e-mail security management, data and communication traffic surveillance, and network segmentation.
- development of holistic information security management including a centralised approach to policy management and adoption (e. g. data security, constant functioning, responses to incidents, and management).
- development of an accountability and awareness culture among employees and students, which includes a strong management system and awareness campaign.

Cheung (2014) defines similar measures mentioning that information security management in higher education institutions should include measures conducted or implemented in eight fields:

- data security,
- security culture and accountability of employees,
- physical security,
- access control,

- communication and commercial process safety,
- information system safety,
- incident management,
- continuous functioning management.

Based on an extensive overview of the literature on the topic of information security incidents and risks in the education branch, Ulven & Wangen (2021) proposed or developed a model of information security elements in higher education institutions. Based on their findings, we created a graphic demonstration of such elements and their connections, shown in table 2.

Table 2: Model of information security elements and information security risks in higher education institutions*

Elements	Incidents		Intruding, infection	Vulnerab. scans	Targeted attacks	fails	Data, equip. theft/loss	kidnapping	Abuse of infrastructure	Internal threats	DDos Attacks
Vulnerabilities	Technical controls		x	x					x		x
	Data control					x					
	Physical controls						x				
	Mobile equip.		x								
	Passwords		x					x			
	Management								x		x
	Awareness		x		x						
	Security culture		x		x					x	
	Resources										
	Complexity		x								x
Motives	Financial		x		x		x				x
	Espionage		x		x			x			
	Grief, revenge								x		
	Activism										
	Opportunism								x		x
	Unintended fails					x					x
	Digital data		x		x			x		x	
	ICT infrastructure		x						x		x
	Personal equip.										
	Physical data							x			
Sources	Data loss		x					x		x	
	Data flow		x							x	
	Loss of access		x			x			x		x
	Data abuse								x		
	Fraud										
	Loss of integrity										
	Loss of equip.										

* The table was made based on data obtained from Ulven & Wangen (2021) including an analysis of 2984 information events noted in higher education between 2017 and 2019 in 10 different sources of literature.

6 Conclusion

Modern times are marked by digitalisation and cybercrime. A pro-active approach to providing information security is of key importance not only for survival but also for the public reputation and competitiveness of an organisation.

Challenges and risks in the field of information security are practically faced by all industries and organisations, disregarding the nature of the branch. There, the higher education branch is no exception, quite the opposite; because of its specific nature (culture of openness, accessibility, and connections), a high amount of confidential data, a high fluctuation of people and a high level of digitalisation and inclusion in cyberspace information security risks are especially high and strongly endanger personal data security, privacy and by this the public reputation of institutions. An overview of the state-of-the-art in the higher education and education branch shows that a lack of adequate technical controls, an underdeveloped security management, a weak awareness of employees and students and a generally low-security culture belong to the main vulnerabilities. Hacker attacks, malware (especially ransomware), DDoS attacks, social engineering attacks (especially phishing attacks), theft and loss of electronic equipment and abuse of user accounts and data most frequently cause incidents. Among the most frequent consequences of incidents, there is a loss, flow or abuse of data and loss of access to them. Among the criminals, financial motives, espionage. Opportunism and also fails of employees prevail. Intentional threats most frequently aim at research and personal data, but also the highly capable infrastructure. In the future, from the aspect of measures, technical security with the implementation of more advanced detection and surveillance mechanisms and from the aspect of management providing for a holistic approach including fostering of awareness and a culture of responsibility on the level of leadership and employees as well as on the level of students must be upgraded.

In a system of providing for information security, it is most important to become aware that social elements are the ones, on which it depends most, whether an organisation will be capable of fighting contemporary threats and defending from cyberattacks. It is a matter of fact that technical measures and control cannot prevent all threats, especially not those connected to the behaviour of users or the use of information systems. Thus, it is for the employees in an organisation to contribute to strong information security or to represent its main vulnerability.

When employees are aware of the rules and threats when they respect policies and act responsibly, they can prevent the realisation of many external threats, but in the opposite case by irresponsible acting and risky behaviour, they make it easy for external threats or enable execution of an attack and by this contribute to the realisation of incidents (Kearney, 2010). People's behaviour is a more unreliable and unpredictable component of information security than technical solutions. Therefore the social sub-system is also much harder to be managed than the technical one. It is therefore not surprising that experts are generally convinced that employees are the weakest part in the information security chain, while higher education institutions are no exception, of course (Hina & Dominic, 2017; Metalidou et al., 2014). From this aspect, it is important that organisations have a holistic management system that also includes organisational and socially oriented activities and measures. In the first place, it is important that a clear vision and a system of rules and accountability is set up and that this is formalised in an information security strategy and policy. Namely, a policy is the backbone of management and the ground of a good information security plan. A system of rules may encompass several kinds of policies, instructions and standing orders, where accountability, demands, processes and control and disciplinary measures are defined. For a successful implementation of policies in practice, it is essential that users get acquainted with it, that they understand the demands and pre-conditions or that it clearly derives from its contents what are their responsibilities and liabilities in the use of information systems and data. But, as Metalidou et al. (2014) stress, the rationality of rules and demands that must have a minimum influence on the productivity and labour of employees must not be neglected because, in the opposite case, employees will find ways of circumvention.

Thus, it is of key importance that rules are clear, unambiguous and understandable. In the same way, it is important that users or employees are trained for execution and motivated for respect. Each employee or user in an organisation should be aware of what responsibilities have been delegated to him or her, how to behave and how to respond in case of facing potential threats (K. Thomson & Niekerk, 2012). In processes of training and awareness building, not only questions on what to do and how to behave must be answered, but also why. Understanding the danger of consequences of information security risks for an organisation can motivate employees to higher compliance (Kearney, 2010). Orshesky (2003) says that the best and easiest way to reach simple, understandable and executable rules and policies for

employees is to include employees already in the development and later implementation of policies at the highest possible level. People, who are part of the process of forming rules, feel more obliged and responsible to follow them and, at the same time, invite others to respect them than when policies are merely dictated or forced upon them.

If organisations wish to reach compliance of user and employees' behaviour with prescribed demands, processes of raising awareness³ and training, as well as fostering legitimacy⁴ of information security among users are inevitable. Since in an organisational environment one must not neglect influence of social learning and group dynamics on people's behaviour, it is of the same importance to develop a positive security culture⁵.

Literature

- Adams, A., & Blanford, A. (2003). Security and Online Learning. In C. Ghaoui (Ed.), *Usability Evaluation of Online Learning Programs* (pp. 331–359). <https://doi.org/10.4018/978-1-59140-105-6.ch018>
- Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1). <https://doi.org/10.1093/cybsec/tyy006>
- Aguilar Quintero, N. A., Velásquez Pérez, T., & Castro Silva, H. F. (2019). Information security model. Case study higher education institution. *Journal of Physics: Conference Series*, 1257(1). <https://doi.org/10.1088/1742-6596/1257/1/012014>
- Allen, J. H., & Westby, J. R. (2007). Governing for enterprise security: Implementation guide. Article 1 - Characteristics of effective security governance. Pittsburgh: Carnegie Mellon University.
- Anderson, R., & Moore, T. (2009). Information security: Where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 367(1898), 2717–2727. <https://doi.org/10.1098/rsta.2009.0027>
- Badic, N., & Lashkari, A. H. (2012). A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. *Journal of Basic and Applied Scientific Research*, 2(9), 9331–9347.
- Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Information & Management Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, 51(1), 138–151. <https://doi.org/10.1016/j.im.2013.11.004>
- Bernik, I. (2014). Cybercrime: The costs of investments into protection. *Varstvoslovje*, 16(2), 105–116.

³ Information security awareness refers to a level of awareness by users on the relevance of information security and knowledge of rules regarding information source security (Khan, Alghathbar, Nabi, & Khurram, 2011).

⁴ Information security is legitimate, when employees understand it as reasonable, needed and wishful and just, and measures are functional and have a minimum influence on the workflow (Son, 2011).

⁵ Information security culture can be defined as value, opinion and behaviour system developed among employees in the use of information, information systems and cyberspace and influencing information security (Da Veiga & Eloff, 2010).

- Bernik, Igor, & Prislán, K. (2016). Measuring Information Security Performance with 10 by 10 Model for Holistic State Evaluation. *PLOS ONE*, 11(9). <https://doi.org/10.1371/journal.pone.0163050>
- Boersma, J., Loke, G., Petkova, V. T., Sander, P. C., & Brombacher, A. C. (2004). Quality of information flow in the backend of a product development process: A case study. *Quality and Reliability Engineering International*, 20(4), 255–263. <https://doi.org/10.1002/qre.551>
- Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, 28(5), 413–422. <https://doi.org/10.1016/j.ijinfomgt.2008.02.002>
- BSI. (2018). ISO 27001 Information Security Features and Benefits. Retrieved from [https://www.bsigroup.com/LocalFiles/en-SG/ISO 27001 SG/ISOIEC 27001-Features-and-Benefits \(SG\).pdf](https://www.bsigroup.com/LocalFiles/en-SG/ISO%2027001%20SG/ISOIEC%2027001-Features-and-Benefits%20(SG).pdf)
- Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance. *Information Security Technical Report*, 17(1–2), 19–25. <https://doi.org/10.1016/j.istr.2011.12.002>
- Buzzelli, M. E. (2021). Protecting and Ensuring Student Privacy. Retrieved from Inside Higher Ed website: <https://www.insidehighered.com/views/2021/04/16/key-steps-take-protect-student-records-and-ensure-cybersecurity-opinion>
- Campbell, S. (n.d.). Cybersecurity in Higher Education: Problems and Solutions. Retrieved from Toptal website: <https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education>
- Center for Internet Security. (2021). CIS Controls. Retrieved from <https://learn.cisecurity.org/cis-controls-download>
- Chang, E. S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3), 345–361. <https://doi.org/10.1108/02635570610653498>
- Cheung, S. K. S. (2014). Information security management for higher education institutions. *Advances in Intelligent Systems and Computing*, 297, 11–19. https://doi.org/10.1007/978-3-319-07776-5_2
- Convention on Cybercrime. (2001). Retrieved from <https://rm.coe.int/1680081561>
- Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers and Security*, 29(2), 196–207. <https://doi.org/10.1016/j.cose.2009.09.002>
- de Oliveira Albuquerque, R., Villalba, L., Orozco, A., Buiati, F., & Kim, T.-H. (2014). A Layered Trust Information Security Architecture. *Sensors*, 14(12), 22754–22772. <https://doi.org/10.3390/s141222754>
- Dell. (2018). Higher Education Security Whitepaper. Retrieved from https://www.delltechnologies.com/asset/en-ca/solutions/industry-solutions/industry-market/dell_hi_ed_security_whitepaper.pdf
- EDUCAUSE. (2019a). Information Security Guide: Effective Practices and Solutions for Higher Education. Retrieved from <https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide>
- EDUCAUSE. (2019b). The EDUCAUSE Information Security Almanac. Retrieved from <https://library.educause.edu/resources/2019/4/the-educause-information-security-almanac-2019>
- EDUCAUSE. (2021). 2021 EDUCAUSE Horizon Report: Information Security Edition. Retrieved from https://library.educause.edu/-/media/files/library/2021/2/2021_horizon_report_infosec.pdf?la=en&hash=6F5254070245E2F4234C3FDE6AA1AA00ED7960FB
- ENISA. (2015). ENISA Threat landscape: Overview of current and emerging cyber-threats. Retrieved from <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014>

- ENISA. (2017). Baseline security recommendations for IoT in the context of critical information infrastructures. Retrieved from https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport
- ENISA. (2018). ENISA Threat landscape report 2017. 15 Top cyber-threats and trends. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport
- ENISA. (2020). ENISA Threat Landscape 2020. Retrieved from <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>
- EU Security Union Strategy. (2020). Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605>
- European Crime Prevention Network. (2016). Cybercrime: A theoretical overview of the growing digital threat. Retrieved from https://eucpn.org/sites/default/files/document/files/theoretical_paper_cybercrime_.pdf
- Eurostat. (2020). ICT usage in enterprises in 2019. Retrieved from <https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f>
- Ezingard, J. N., McFadzean, E., & Birchall, D. (2005). A model of information assurance benefits. *Information Systems Management*, 22(2), 20–29. <https://doi.org/10.1201/1078/45099.22.2.20050301/87274.3>
- Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information Sciences*, 256, 57–73. <https://doi.org/10.1016/j.ins.2013.02.036>
- FireEye. (2014). Why Cyber Attackers Are Targeting Higher Education, and What Universities Can Do About It. Retrieved from <https://www.fireeye.com/current-threats/threat-intelligence-reports/wp-storming-the-ivory-tower.html>
- Fishman, T., Rudnicki, R., & Grama, J. L. (2021). NIST Special Publication 800-171 for higher education A guide to helping colleges and universities comply with new federal regulation. Retrieved from Deloitte Insights website: <https://www2.deloitte.com/us/en/insights/industry/public-sector/protecting-classified-uncontrolled-information-higher-education.html>
- Furnell, S., & Moore, L. (2014). Security literacy: The missing link in today's online society? *Computer Fraud and Security*, 2014(5), 12–18. [https://doi.org/10.1016/S1361-3723\(14\)70491-9](https://doi.org/10.1016/S1361-3723(14)70491-9)
- Goodyear, M., Portillo, S., Goerdel, H. T., & Williams, L. (2010). Security officers: Strengthening cybersecurity series. Washington: IBM Center for The Business of Government.
- Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management and Computer Security*, 16(4), 377–397. <https://doi.org/10.1108/09685220810908796>
- Hina, S., & Dominic, D. D. (2017). Need for information security policies compliance: A perspective in Higher Education Institutions. *International Conference on Research and Innovation in Information Systems, ICRIS*, 1–6. <https://doi.org/10.1109/ICRIS.2017.8002439>
- Hommel, W., Metzger, S., & Steinke, M. (2015). Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization. *EUNIS Journal of Higher Education IT*, (2015/3), 1–12.
- Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys*, 52(2). <https://doi.org/10.1145/3303771>
- Impact. (2021). 15 Cybersecurity in Education Stats You Should Know for 2020. Retrieved from <https://www.impactmybiz.com/blog/cybersecurity-in-education-stats/>
- Interpol. (2021). Cybercrime: Cyberattacks know no borders and evolve at a rapid pace. Retrieved from <https://www.interpol.int/Crimes/Cybercrime>

- ISO/IEC 27000:2018. (2018). Information technology - Security techniques - Information security management systems - Overview and vocabulary. Geneva: International Organization for Standardization, International Electrotechnical Commission [ISO/IEC].
- ISO/IEC 27005:2018. (2018). Information technology - Security techniques - Information security risk management. Geneva: International Organization for Standardization, International Electrotechnical Commission [ISO/IEC].
- Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, 23(2), 139–154. [https://doi.org/10.1016/S0268-4012\(02\)00105-6](https://doi.org/10.1016/S0268-4012(02)00105-6)
- Kearney, P. (2010). *Security: The Human Factor*. Cambridgeshire: IT Governance Pub.
- Khan, B., Alghathbar, K. S., Nabi, S. I., & Khurram, M. (2011). Effectiveness of information security awareness method based on psychological theories. *African Journal of Business Management*, 26(5), 10862–10868.
- Klimoski, R. (2016). Critical Success Factors for Cybersecurity Leaders: Not Just Technical Competence. Retrieved from People + Strategy Journal website: <https://www.shrm.org/executive/resources/people-strategy-journal/Winter2016/Pages/success-cybersecurity.aspx>
- Lađići, T. (2019). Cyber: How big is the threat? Retrieved from <http://www.europarl.europa.eu/thinktank>
- Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of it business value. *MIS Quarterly: Management Information Systems*, Vol. 28, pp. 283–322. <https://doi.org/10.2307/25148636>
- Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Giannakopoulos, G., & Skourlas, C. (2014). Human factor and information security in higher education. *Journal of Systems and Information Technology*, 16(3), 210–221. <https://doi.org/10.1108/JSIT-01-2014-0007>
- Mishra, S., & Chasalow, L. (2011). Information Security Effectiveness: A Research Framework. *Issues in Information Systems*, XII(1), 246–255. https://doi.org/10.48009/1_iis_2011_246-255
- Morgan, S. (2020). Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. Retrieved from *Cybercrime Magazine: Special Report: Cyberwarfare In The C-Suite* website: <https://cybersecurityventures.com/hackreport-cybercrime-report-2016/>
- Morphisec. (2020). Education Cybersecurity Threat Index. Retrieved from <https://engage.morphisec.com/education-cybersecurity-threat-index>
- Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). NIST Special Publication 800-12 Revision : An Introduction to Information Security. <https://doi.org/10.6028/NIST.SP.800-12r1>
- Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. *International Journal of Information Management*, 49(April), 208–216. <https://doi.org/10.1016/j.ijinfomgt.2019.04.010>
- Orshesky, C. M. (2003). Beyond technology – The human factor in business systems. *Journal of Business Strategy*, 24(4), 43–47. <https://doi.org/10.1108/02756660310494872>
- Osborne, M. (2006). *How to cheat at managing information security*. Rockland: Syngress Publishing.
- Pesante, L. (2008). *Introduction on information security*. Pittsburgh: Carnegie Mellon University.
- Pfleeger, C. P., & Pfleeger, S. L. (2006). *Security in computing* (4th ed.). Upper Saddle River: Prentice Hall.
- Pfleeger, S. L., & Stolfo, S. J. (2009). Addressing the insider threat. *IEEE Security and Privacy*, 7(6), 10–13. <https://doi.org/10.1109/MSP.2009.146>
- Prislán, K., & Bernik, I. (2019). *Informacijska varnost v organizacijah*. Maribor: Univerzitetna založba Univerze v Mariboru.
- Prislán, K., Mihelič, A., & Bernik, I. (2020). A real-world information security performance assessment using a multidimensional socio-technical approach. *PLOS ONE*, 15(9). <https://doi.org/10.1371/journal.pone.0238739>

- Proofpoint. (2021). Threat report: State of the Phish Report. Retrieved from <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>
- Schatz, D., & Bashroush, R. (2017). Economic valuation for information security investment: a systematic literature review. *Information Systems Frontiers*, 19(5), 1205–1228. <https://doi.org/10.1007/s10796-016-9648-8>
- Seese, M. (2009). Scrapy information security: The easy way to keep the cyberwolves at bay. Silicon Valley: Scrapy About.
- Sethuraman, S., & Adaikkappan, A. (2009). Information security program: Establishing it the right way for continued success. *ISACA Journal*, 5, 1–7.
- Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information and Management*, 48(7), 296–302. <https://doi.org/10.1016/j.im.2011.07.002>
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly: Management Information Systems*, 34(Spec. Issue 3), 503–522. <https://doi.org/10.2307/25750689>
- Tayaksi, C., Ada, E., Kazancoglu, Y., & Sagnak, M. (2021). The financial impacts of information systems security breaches on publicly traded companies: reactions of different sectors. *Journal of Enterprise Information Management*. <https://doi.org/10.1108/JEIM-11-2020-0450>
- The CERT Insider Threat Center. (2016). Common Sense Guide to Mitigating Insider Threats, Fifth Edition. Retrieved from <https://www.odni.gov/files/NCSC/documents/nittf/20180209-CERT-Common-Sense-Guide-Fifth-Edition.pdf>
- The EU's Cybersecurity Strategy for the Digital Decade. (2020). Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164
- Thomson, K. L., & von Solms, R. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud and Security*, 2006(5), 11–15. [https://doi.org/10.1016/S1361-3723\(06\)70356-6](https://doi.org/10.1016/S1361-3723(06)70356-6)
- Thomson, K., & Niekerk, J. Van. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management and Computer Security*, 20(1), 39–46. <https://doi.org/10.1108/09685221211219191>
- TopLine Comms. (2020). UK university ransomware FoI results. Retrieved from <https://toplinecomms.com/insights/uk-university-ransomware-foi-results>
- Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, 13(2), 1–40. <https://doi.org/https://doi.org/10.3390/fi13020039>
- Verizon. (2019). Insider Threat Report. Retrieved from <https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf>
- Verizon. (2021). Data breach investigation report. Retrieved from <https://www.verizon.com/business/resources/reports/dbir/>
- von Solms, B. (2001). Information security - A multidimensional discipline. *Computers and Security*, Vol. 20, pp. 504–508. [https://doi.org/10.1016/S0167-4048\(01\)00608-3](https://doi.org/10.1016/S0167-4048(01)00608-3)
- von Solms, B. (2010). The 5 Waves of Information Security-From Kristian Beckman to the Present. In K. Rannenber, V. Varadharajan, & C. Weber (Eds.), *Security and Privacy – Silver Linings in the Cloud*. SEC 2010. IFIP Advances in Information and Communication Technology, vol 330. (pp. 1–8). https://doi.org/https://doi.org/10.1007/978-3-642-15257-3_1
- Vrhovec, S., & Mihelič, A. (2021). Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers and Security*, 106. <https://doi.org/10.1016/j.cose.2021.102309>
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18(2), 101–105. <https://doi.org/10.1057/ejis.2009.12>
- Whitman, M. E., & Mattord, H. J. (2012). *Principles of information security* (4th ed.). Boston: Course Technology, Cengage Learning.

Annex A: Standards and Guidelines

ISO/IEC 27000 (*Information technology – Security techniques – Information security management systems – Overview and vocabulary*). Description: textual, glossary giving a general overview of the information security management system and explanations on expert terminology and definitions usually utilised in the ISO 27000 standards series.

ISO/IEC 27001 (*Information technology – Security techniques – Information security management systems – Requirements*). Description: the standard represents demands for formation, execution, maintenance and permanent improvement of the information security management system in organisations - ISMS. ISMS is a general management framework enabling an organisation to identify, analyse and handle information security risks. In case of a certification, organisations must determine how specific fields and controls defined in the standard are dealt with.

ISO/IEC 27002 (*Information technology – Security techniques – Code of practice for information security controls*). Description: the standard contains instructions widening and thoroughly describing information security management control defined in the standard ISO/IEC 27001. It is a code of conduct used by organisations as guidelines for obtaining the ISO/IEC 27001 certificate.

ISO/IEC 27003 (*Information technology – Security techniques – Information security management systems – Guidance*). Description: the standard includes directives for information security managers on approaches and ways of planning and execution of implementation of the ISMS system and recommendations after ISO/IEC 27001.

ISO/IEC 27004 (*Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation*). Description: Gives directives for assessment of success and effectiveness of the information security management system (processes, surveillance and control).

ISO/IEC 27005 (*Information technology – Security techniques – Information security risk management*). Description: the standard gives directives for mastering information security risks and supports general concepts determined in ISO/IEC 27001. The standard gives starting points to be followed by an organisation in formation of its risk management system.

ISO/IEC 27031 (*Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity*). Description: the standard describes how to provide for readiness for constant operation on ICT level. It is about an upgrade of the incident management system.

ISO/IEC 27032 (*Information technology – Security techniques – Guidelines for cybersecurity*). Description: the standard gives directives for providing for and development of cybersecurity in organisation in fields, as there are: information security, network and internet security, critical and key infrastructure security.

ISO/IEC 27035-1 and ISO/IEC 27035-2 (*Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management / Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*). Description: a standard for incident management composed of two parts. The first part of the standard defines basic concepts and defines key phases of reaction to incidents (detection, reporting, assessment, response). The second part contains directives and instructions for formation of a plan and preparation of s response, together with good practices.

ISO 22301 (*Security and resilience – Business continuity management systems – Requirements*). Description: a standard for constant activity performance, listing pre-conditions for planning, execution, management, surveillance and maintenance of a system in an organisation for protection from interruption of activity. It describes how to respond to events and how to tackle renewal of activity and gives directives for risk reduction, as well. Demands are general and meant for use in all organisations. The range of these demands depends on the environment and complexity of an organisation.

ISO/IEC 15408-1 (*Information technology – Security techniques – Evaluation criteria for IT security*). Description: the standard determines security matters and common criteria for assessment or testing of information security technology. It describes criteria to be met by computer products tested and certified for security aspects.

Standard of Good Practice (publisher: Information Security Forum - ISF). Description: Standard of Good Practice is meant for leaders and managers of information security, IT managers, internal and external auditors and IT suppliers as a practical handbook for the detection and management of risks in the field of information security in organisations and their supply chains.

Cybersecurity Framework (publisher: NIST). Description: a framework for providing for cybersecurity, giving directives to organisations in the formation of cybersecurity and cyber risk mastering based on existing standards, instructions and good practice. The framework is mainly meant for systems of critical infrastructure. It gives a taxonomy of wishful organisational states and results and describes the realisation of these goals with respect to normative demands regarding the protection of privacy and personal data.

Special Publications 800 series (publisher: NIST). Description: a series of more than 190 standards or publications handling most various aspects of providing for information and cybersecurity (from general concepts to technical solutions), or giving directives for specific branches.

IASME (*Information Assurance for Small to Medium-sized Enterprises Governance Standard*). Description: the standard describes criteria for data security in smaller enterprises.

COBIT 5 for Information Security (publisher: ISACA, *Control Objectives for Information and Related Technology - COBIT: A business framework for the governance and management of enterprise IT*). Description: commercial framework for leading and managing information security technologies in organisations. It gives concrete instructions regarding formation of a proper organisational structure and culture being the base for a high level of information security. It includes a methodology for assessment and evaluation of information security maturity.

PAS 555 (publisher: British Standard Institution – BSI, *Cyber security risk. Governance and management. Specification*). Description: a general business model for information security management in organisations and a complete partner chain. It contains as technical as well as user and organisational aspects. It is the result of an initiative by larger IT enterprises. It describes roof pre-conditions and fields to be regulated for providing for a holistic approach to security and an according interconnection between the fields.

BS 10012 (publisher: British Standard Institution – BSI, *Personal Information Management System*). Description: recommendations for providing for privacy and personal data security in line with demands by General Data Protection Regulation (GDPR).

BS 7799 (publisher: British Standard Institution – BSI, *Information Security Risk management*). Description: the standard describes processes and procedures relevant for information security risk management in organisations. Directives are compliant with ISO/IEC 27001 and general Data Protection Regulation (GDPR).

BSI-Standard 100-3 (publisher: Bundesamt für Sicherheit in der Informationstechnik – BSI, *Risk analysis based on IT-Grundschutz*). Description: the standard presents a methodology and a process for risk assessment in the field of data processing in line with the classification of threats and risks defined in the IT-Grundschutz catalogue (Germ. GSK).

CYBERSECURITY FOR ONLINE EDUCATION

MARKO KOMPARA, MARKO HÖLBL

University of Maribor, Faculty of Electrical Engineering and Computer Science
marko.kompara@um.si, marko.holbl@um.si

Abstract Online education has become very popular, and like anything online, it is also prone to cyberattacks from malicious adversaries. Cybersecurity in online education is important primarily because of the participants' sensitive personal information such systems hold and the damage and impact a successful attack could cause (e.g., the loss of progress and any grades students have received so far in their education and potentially lost records of graduates). This work presents the cybersecurity challenges and problems in online education. It shows the most relevant issues for education attendees and education providers. The manual introduces some important properties of a security system and gives some recommendations on how to achieve them. The content is aimed more at personnel that manage or want to establish an online learning environment. Still, the users (students or teachers) can also get useful information on how to design their passwords and how to use them, multi-factor authentication, and how their human nature puts them at risk of being exploited.

Keywords:

cybersecurity,
online learning,
online education,
e-learning,
learning
management
system

1 Introduction

Online learning allows everyone the opportunity to improve their education. Online learning is a form of distance learning where the participants and the instructors are physically not together, and the interaction is mostly asynchronous. By leveraging information and communication technologies, online learning offers advantages over traditional learning, like learning at any time and (almost) anywhere. This eliminates scheduling and distance problems that are often limiting in the modern, fast-paced, globalised world. It also improves access to education and training. It reduces the costs for the organisations providing the education (e.g., no need for physical classrooms) and students (e.g., no travelling to school or renting a place to stay while at school), which also removes socioeconomic status barriers. All these advantages and the flexibility of online learning are often the driving motivators for choosing online education over traditional in-person forms of education.

Online learning is typically implemented using a Learning Management System (LMS). LMS is in some ways similar to much more common Content Management Systems (CMS) that are used for managing websites. A learning management system supports the administration, documentation, tracking, reporting, automation, and delivery of educational courses or training programs. An LMS provides virtual classrooms in which students and teachers interact. It hosts educational material and distributes it to students over the Internet (in the form of a webpage). Learning materials can include text, images, audio and video presentations, and link to other (outside) resources. The teachers manage the virtual classroom, upload any learning materials, assign students their assignments, and guide students in their work. To breach the communication challenge of distance learning, LMS systems provide good communication links between teachers and students. An example of such a learning management system is Moodle, which is the main topic of this manual.

However, like everything else that functions over the internet, online learning is also threatened by malicious actors. The main risks involve loss of confidentiality, availability, trust, exposure of critical data, and vandalism of the provided service. To defend against these risks, cybersecurity must be employed. Cybersecurity is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks.

Table 1 presents security issues in online learning and consequently relevant in learning management systems. The table is based on the work done by S. M. Furnell and T. Karweni (2001) and, in addition to the security issues, also shows which are relevant for the system's majority users (i.e., students) and which are predominately crucial for the organisation providing and managing an education program together with the learning management system.

Table 1: Security issues in online learning and whether they are essential for students and the education provider.

Security Issues	Student Interest	Education Provider Interest
Privacy and confidentiality of personal data	✓	✓
Security of service usage		
– Authentication and accountability	✓	✓
– Access control		✓
– Protection from malware		✓
Human aspects (e.g., phishing)	✓	✓
Security of payment (i.e., enrolment fees, if any)	✓	✓
Security of data		
– Authentication	✓	✓
– Confidentiality	✓	✓
– Integrity	✓	
– Non-repudiation	✓	✓
Secure communication	✓	✓
Security of educational materials		
– Prevention of unauthorised access		✓
– Prevention of unauthorised distribution		✓
– Software licence control		✓
Confidentiality and secure conduct of knowledge assessments	✓	✓
Proof of completing the education		
– Verification of education provider	✓	✓
– Verification of the integrity		✓
Reliability and availability of education environment	✓	✓
Maintenance		✓
Backups	✓	✓

The remainder of this manual addresses issues raised in Table 1 and what cybersecurity techniques and solutions can be applied to protect against them. Not all the problems mentioned in the table will be directly addressed, as some are not primarily in the domain of education providers (e.g., security of payments or

software licence control), and others have the same underlying technologies (e.g., access control and prevention of unauthorised access).

In this manual, we also wish to support some other work done in the Cyber F-IT project. Other outputs include information on privacy, information security management in higher education, and configuration and use of Moodle learning management system. This manual aims to give the readers some context to how privacy and security are connected but mainly presents some basic security concepts and mechanisms that must be put in place to secure an environment, such as an LMS. With this knowledge following the options shown in the configuration process of Moodle platform, readers will better understand what individual options are for and why they are required. Most of this manual would be more interesting to education providers; however, end-users, like students and teachers, could also gain valuable information from it. For them, we recommend reading sections 3.1, 3.2, 5, and 7.

2 Privacy

The educational environment is full of valuable personal data. It is the institution's responsibility that is providing the education not to exploit this data (but to use it only for its intended purposes) and to protect it from other malicious entities. Privacy relates to one's right to control personal information and how it is used. Security, on the other hand, is about how data is protected. The two are connected because cybersecurity is what protects an individual's privacy (i.e., personal data). Personal data is any data relating to an identifiable person. A privacy policy is one of the most important aspects of ensuring user privacy. This manual defines all the ways in which an organisation (i.e. education provider) gathers, uses, discloses, and manages users' (i.e., students') data. Especially in more recent times, the protection of personal information has become a big issue, and legislation was put in place to ensure that anybody processing personal data keeps them safe in suitable ways and uses them in a responsible manner. You can learn more about this in the chapters Personal Data Security (Directives of Education Institutions and Students) and Information Security Management in Organisational Settings and Higher Education Institutions.

3 Authentication, Authorisation, and Access Control

Authentication is the process of confirming somebody's identity. The most common authentication method is the username and password combination, which we discuss in more detail below. However, there are others: biometry, smart cards, one-use tokens, etc. Authentication credentials can be done based on what one knows (e.g., password), what they are (e.g., fingerprint), and/or what they have (e.g., a smart card). The problem, especially when it comes to examinations in an online setting, is the prevention of possible sharing of credentials to have somebody else taking the exam instead of the designated participant. This is most serious in the case of the "what you know" and "what you have" credentials that can be more easily shared but are not entirely avoided in the case of "what you are" credentials either (e.g., the participant takes the examination together with the helper). When it comes to examinations, the authentication process is, therefore, often more complex and involves sharing a live feed of the participant's web camera (for the duration of the examination) together with showing a form of personal identification. Ultimately, this problem of verifying whether or not the right person did the assignment/examination is one of the significant reasons why remote learning has not spread as much for formal education purposes.

The authorisation comes after authenticating a user and defining what a specific user has access to. Participants need access to all their courses, learning materials, any work they have submitted or grades they have received, etc. Still, at the same time, they must not have access to the back end of the used education platform, assignments their classmates might have submitted, grades they might have received, classes they are not enrolled in, etc. For teachers, it is similar, but they must have access to all the submitted work and grades of everybody in their course (usually, they should not get access to courses they do not teach), and they also get the option to add and change the content of the course as well as give grades etc. Course administrators (not system administrators) usually do not get access to course content, but they can add and remove participants and teachers from courses. Finally, system administrators have access to the back end (e.g., configuration) of the platform and have, in general, the highest authorisation level. Strong authentication practices are especially important for system administrator accounts because unauthorised access can cause the most damage. It is, therefore, the best practice to enable all the available security features for the administrator accounts.

Access control is the broadest concept of the three presented here. It includes authentication and manifests the rules set by the authorisation and many more things. At its simplest, access control protects front-end and back-end data and system resources. An access control scheme should protect against unauthorised viewing or any form of data changes. Access control mechanisms can also help limit malicious code execution or unauthorised actions by an attacker exploiting infrastructure vulnerabilities. Access control can be based on physical attributes, sets of rules, lists of individuals or systems (i.e., access list), or other, more complex means (e.g., intrusion detection system). Role-based authorisation is the most commonly used model of restricting the system access of unauthorised users. It allows defining groups, assigning users into groups or even groups into other groups. This model allows for flexible and granular control of the access rights of each user. The permissions themselves (i.e., what somebody can do and access) are assigned roles (teacher, student, course administrator, unregistered user, system administrator, etc.). System users are assigned particular roles, from which they acquire the permissions to perform particular system functions. Since the users do not have the permissions directly assigned to them, management of individual user rights is simpler and more reliable from a management standpoint.

3.1 Passwords

Passwords are the prevalent authentication method because they are the easiest for developers to implement and users to understand and use. However, some conceptual weaknesses are associated with using passwords (namely, when they are poorly selected, easily guessed, etc.). The U.S.A.'s National Institute of Standards and Technology (NIST) regularly updates its recommendations for creating and managing passwords (see NIST Special Publication 800-63B - Digital Identity Guidelines: Authentication and Lifecycle Management by Grassi, P. et al.). In one of the recent shifts in the paradigm of password security, they have suggested that users focus on password length over complexity (combinations of special characters, numbers, lowercase or capital letters) because complex passwords are hard to remember. Consequently, users tend to achieve complexity in predictable ways (e.g., adding the number 1 at the end of a password). One way to achieve length is with nonsensical passphrases, where words are in a sequence with no meaning. For the same reason, NIST no longer recommends strict character composition rules when creating a password. However, they recommend regularly comparing passwords (or

at least any new passwords) to a list of compromised passwords to identify already revealed and weak passwords. Nevertheless, the recommended minimum length of a password is still eight characters. While regular changes of passwords were recommended in the past, this is no longer the case. This makes users less likely to remember their passwords after changes and instead start using the same passwords with minor alterations. The minimum protection of the stored passwords should include hashing and the use of salts (salt is a random value that prevents identical passwords from hashing into the same value and specific attacks). Additionally, NIST suggests locking a user out of the system if they use an incorrect password too many times (e.g., after three unsuccessful tries, a user cannot try again for one minute), allowing emojis, ASCII, and Unicode characters in passwords, and allowing copy and paste functions in the password fields to make using password managers and multi-factor authentication, which we will both address shortly, more convenient.

Finally, although you can use technical measures to ensure users choose robust passwords, it is impossible to control what users do with them. They can write it on paper next to their computer, share it with others, or use it for other accounts. The latter is dangerous, as using the same password across multiple accounts will compromise all of them if any of the services using the same passwords are breached. This means that if you use the same password for accessing your library and e-mail account if somebody breaches the security of the library (which should be a lot easier than the servers of a large e-mail service provider – e.g., Google) and steals the password, they can use that information to gain access to your e-mail account. Educating the users is the only real solution to prevent such bad practices. Therefore, users should be educated (on how) to create strong passwords, not to write them anywhere accessible, and never to reuse the same password.

One of the best solutions for remembering or, better said, storing a large number of passwords and any other authentication-related information (e.g., private keys) are password managers. A password manager is a software solution (online or local) that stores all your credentials (typically username and password) in a secure way by encrypting them. Access to the list is protected in any possible ways we have discussed (password, fingerprint, multi-factor authentication, etc.). The “master password” that protects access to all the other passwords must be very secure (for obvious reasons). The advantage of such a setup is that the user must only remember

one very good password to gain access to any number of services that use a different password stored with the manager. Password managers can also generate completely random values for users to use as passwords (random values are the best possible passwords). There is no longer a need for such passwords to be memorised.

A final consideration when using passwords in an educational setting is the possibility of sharing a password. A student can give their password to somebody else, who can log in as them and participate and/or submit any assignments, examinations, etc., in the credential holder's name. Multi-factor authentication is one way to make this more challenging (how much harder credentials sharing becomes depends on the factors used).

3.2 Multi-Factor Authentication

Multi-factor authentication (MFA) is authentication using at least two different factors (what you know, what you are, and what you have). Two-factor authentication (2FA) is basically the same, but precisely two factors are used. Nowadays, if MFA is used, it is almost always 2FA. Typically, the first factor is a password or a PIN (something you know), and the second is usually a bank card, SMS, or a code generated by a mobile app (what you have - i.e., your mobile device). Using fingerprints, retina scans, etc. (what you are) is an option, but it is less often used because additional hardware is required (with higher cost).

Multi-factor authentication is a good way to mitigate the risk and reduce the chances of compromised credentials. For example, let us look at a password and app code combination. Even if the site itself is compromised or a password is obtained from somewhere else, the attacker cannot log in because while they can provide the appropriate username and password, they cannot provide the code generated on the mobile device. The stolen password becomes useless (unless the attacker steals the mobile device as well, but that is not a scalable attack and, therefore, not a serious threat to most people). Meanwhile, the system administrators can still detect unsuccessful attempts to log in and ask a specific user to change their password or all of their users if their system was compromised and all the passwords leaked.

4 Confidentiality, Integrity, and Non-Repudiation

Confidentiality, Integrity and Availability (CIA) are considered to be the three primary pillars of information security. Confidentiality is the principle of keeping data confidential/private. One part of this is the previously discussed access control, where access to data is limited. The second part deals with situations where anybody can access information, but it must remain confidential. In this case, confidentiality is achieved with encryption. Confidentiality is important in any system, and the same is true for online learning systems. Any work students submit should stay confidential (except for teachers grading the assignment), and any grades received should not be publicly accessible (even to other students).

The integrity of data prevents unauthorised modifications to data. Technically this is implemented in a way that any change is easily detectable (because it is impossible to prevent changes in some environments). Integrity is essential for establishing trust in the system. Students, for example, must be assured about the integrity (i.e., correctness) of grades or that assignments that they submitted were not changed (on purpose or by mistake) during transmission or while on the server. To guarantee confidentiality and integrity, the security of network communications is paramount.

Even though confidentiality and integrity of data are important, the data or service is of little use if it is unavailable. We will discuss availability together with reliability shortly.

Non-repudiation ensures that users cannot deny they have carried out an action. For example, if a teacher were to remove a student from a course, it should be possible to track who removed them. The audit trail (e.g., log files) must be reliable and tamper-proof to ensure integrity and non-repudiation.

5 Secure Communications

We have discussed how the security of data at rest (e.g., on a system) is important. However, the security of data while in transit is just as important, if not even more so, because while data is in transit (e.g., on the Internet), it is not under any ones' control, and it can be eavesdropped on or modified. Therefore, using methods that ensure confidentiality and integrity to prevent this from happening is essential. The

standard way to access online education is over HTTP (Hypertext Transfer Protocol). However, this protocol only concerns how data is transported between the client (e.g., a browser of a student, teacher, or system administrator) and the server. HTTPS (Hypertext Transfer Protocol Secure) should be used to protect the data while in transit. This is basically the same as the original protocol but also provides data confidentiality, integrity, and authentication. HTTPS is the standard method used today. Anyone using the Internet (for education or otherwise) should stick to web pages using this protocol, especially if any personal information is sent to a web page or the page requires a login.

The protocol used within the HTTPS that protects communication through end-to-end encryption is called Transport Layer Security (TLS). For TLS to work to its full potential, the service providers must obtain a TLS certificate, which helps authenticate the server (clients are typically not authenticated in this way). This helps prevent fake websites from pretending to be legitimate. Users can check this in their browsers by clicking on a lock icon next to their URL bar. Systems like those for online learning can have connections to multiple external systems or databases containing information on all the students and teachers, their activities on the platform, course catalogues, etc. Any such connections also must be protected in the same way.

6 Reliability and Availability

Reliability is defined as the probability of a system or a system part performing its intended function under stated conditions without failure for a given period (Stallings, 2023). In other words, the reliability of a system supporting online learning is the property of a system to produce consistently correct responses/outputs to given actions/inputs. Reliability in a learning environment can also be looked at from the perspective of course materials (they are correct, current, and relevant), but that is fundamentally a question of data integrity (the materials were not corrupted) and the quality of data itself.

Availability is the third pillar of the CIA triad mentioned previously. Availability is the assurance that the environment or service (e.g., remote learning) is accessible (to authorised users) whenever required (Stallings, 2023). One of the main advantages of online learning (if it is not in person) is that the time and work distribution is

largely flexible to the needs and requirements of participants/students. For this to be a realisable advantage, availability is essential. Access to study materials and the possibility to submit any assignments must be available at all times for online education to reach its full potential and to give all participants equal possibilities of engagement. For example, online learning is desirable to people who already have jobs or other commitments that do not allow them to attend a class every day. Availability of the course allows them to do their work after they finish their jobs, in the evenings or at the weekends and can therefore be extremely important for online learning. Disruption of availability (even for a short time) can cause a loss of revenue, customer dissatisfaction, and/or reputation damage. The majority of threats to availability are not malicious and can include any number of hardware, software and/or network issues. A typical attack that targets the availability of resources is a Denial of Service (DoS) attack, which we will discuss in more detail later. Measures to ensure better availability include backups, hardware, systems and potentially location redundancy, firewalls, network monitoring and appropriate routing, etc.

7 Human Aspects

In cybersecurity, it is often said that people are the weakest link in the security of a system. This is because while the technical security of systems is constantly improving, we cannot really improve people other than educating them on the proper ways to use a system and how to avoid behaviours that could put them or the system they use at risk. However, in the end, users still try to make their life easier when possible or do what they believe is the right thing at a given moment, even if it is not. Attackers are well-aware of this and will try and exploit these characteristics.

We have already discussed one good example of this in the section on passwords. Even though rules on how passwords should be constructed and stored are well-known, users often ignore them because it is easier to remember a simpler password, write it on a piece of paper next to the computer, or use the one and the same password for everything. As a result, attackers successfully guess passwords (because users use simple and similar passwords) and use discovered passwords to attack other services the user might use.

The second major way attackers exploit human nature is through social engineering. Social engineering is the psychological manipulation of people to do what the attacker wants or divulge confidential information (Stallings, 2023). Examples of social engineering include scareware (using false alarms and fictitious threats), pretending to be an authority, pretending there is an emergency, impersonating specific people, etc. Possibly the most common, however, is phishing. Users should be wary of unsolicited messages, links and attachments in e-mails from an unknown source or offers that are too good to be true, etc.

7.1 Phishing

Phishing is a type of social engineering attack where the attacker sends the victim a deceptive message to have them reveal some information or cause them to deploy malicious software. Phishing attacks are untargeted (similar targeted attacks are called spear phishing), meaning they are sent to many people simultaneously. Their aim is not to fool everybody or even a majority, but a small success rate is already good enough because the messages are sent to so many people. Phishing can be done over voice (e.g., phone calls), social media, SMS, and most commonly, e-mail. Phishing e-mails often have spelling errors, poor grammar, bad graphic design, are very generic or get your name wrong (typically based on the e-mail address). However, not all phishing suffers from these deficiencies; therefore, vigilance is still key.

Phishing is often the first step of an attack, used to convince a user to deploy some other malicious software on their device and then use that malware to do the actual damage. This can include traditional viruses and worms, cryptocurrency-mining malware, lately prevalent ransomware (it renders the victim's computer files useless by encrypting them and demands ransom for their decryption), etc.

Organisations can do a lot to alleviate the risks of phishing (e.g., firewalls, spam filters, required MFA, etc.); however, some messages will almost certainly still make it to the end-users. To protect themselves, users should:

- verify the sender by checking their e-mail address,
- check any links before clicking them,

- do not provide any personal information if they do not trust the source,
- do not rush or panic react to a message (e.g., quickly opening an attachment because the message was marked as urgent),
- delete any received phishing messages without interacting with them (e.g., opening attachments or clicking on links) and report them (this can help prevent others from being affected by the same attack).

8 Maintenance

When any vulnerabilities are discovered, patches (i.e., updates that address security vulnerabilities) are made. If the system producer discovers the vulnerability, users will probably have some time to update their systems before the vulnerabilities are announced to the public. However, when malicious attackers discover vulnerabilities, the time it takes to produce and apply patches is critical in limiting the damage.

Modern LMS require many other components like operating systems, web services, content management systems, databases, and plugins. A typical Moodle install will have a Linux operating system, web server software, PHP, MySQL and any number of plugins. System administrators must constantly monitor, maintain, and upgrade all components to ensure everything works as it should. They should pay special attention to possible security patches and apply them as soon as possible. When there are major upgrades, a good option is to first test them in a staging environment before applying them to the live environment, just in case the new update breaks something.

Good maintenance practices extend beyond the web servers, as switches and firewalls should also be maintained with the same vigour and attention. Special attention should also be paid to plugins and extensions, which are often forgotten. They are usually not professional products created by an organisation that regularly updates them but hobby projects created by individuals. As such, they should be regularly checked, any plugins/extensions no longer in use should be removed, and unnecessary plugins/extensions should not be installed.

9 Backups

Backups are the ultimate recovery solution after a system has been compromised and, as such, are extremely important. The safest mindset is to assume you will be hacked or there will be some crucial hardware malfunction or a natural disaster, after which the only solution to re-establish the environment as it was before the event will be from a backup. A bug in the LMS can also cause a loss of data. In any of these cases, it is very important to recover all the learning materials, any work students have done so far, and their grades. If any of this data is lost, it would mean a lot of lost effort for the students and teachers and a big reputation hit for the educational institution.

A sound backup system regularly saves backups in different locations and frequencies. Other locations are required so that, for example, one natural disaster does not destroy all the backups. Meanwhile, having backups from different time points is necessary because compromises are not always immediately discovered. Therefore, a backup from yesterday, a week or a year ago might be necessary to establish an environment where the cause for the ultimate failure was not already present. However, just having backups is not enough. Procedures for testing the backups and recovering from them in a timely fashion are necessary for backups to work and be useful when you need them.

10 Malware

Malware (a portmanteau of malicious software) is software intentionally designed to be harmful to computers and computer systems. Many types of malware are based on their operation and end goal.

Viruses were the original malware back when all malicious programs were called viruses. They are self-replicating programs that infect files (i.e., imbed malicious code into existing files).

Worms also self-replicate but do not require a host program to do so. They spread over networks and can potentially infect all the devices within a network.

Trojans disguise themselves as legitimate and useful non-malicious software to gain access to a system. Once there, they typically deploy their malicious functions while still performing their “useful” function to avoid arousing suspicion. Trojans typically do not self-replicate.

Spyware runs secretly while collecting and reporting any information on the system or about the activities of the users. They usually target sensitive information (e.g., personal information, financial information, or credentials).

Adware also collects information on the user but primarily to display advertisements that the users are more likely to be interested in. Adware can be the least dangerous type of malware on the list, but it can open doors for other malicious software and hinder the performance of the infected device.

Ransomware encrypts files on the system after gaining access to it. Users must pay a ransom if they want to recover inaccessible data. Data is typically unlocked after paying the ransom, but not always.

A variety of solutions are used to detect and prevent malware. The most basic one, and the one everybody can and should have on their machine, is the antivirus/antimalware program. Other measures (more interesting for use in organisations – e.g., education providers) include firewalls, network intrusion prevention systems, deep packet inspection, unified threat management systems, antivirus and anti-spam gateways, virtual private networks, content filtering, and data leak prevention systems.

11 Vulnerabilities/Attacks

There are many vulnerabilities and possible attacks. This section will briefly introduce some of the more common types of vulnerabilities/attacks.

A brute force attack is an attack of guessing. It is the most basic of attacks and very inefficient. Still, brute force attacks can offer good results when the security level is small enough or the secret is predictable enough. Brute force attacks are typically done on passwords but can be done on all types of secrets (e.g., PINs or cryptographic keys). The best defence against a brute force attack is to limit the

number of attempts in a given time. For example, suppose an attacker (or a legitimate user) enters the wrong password five times. In that case, the account is automatically locked for one minute, and no more attempts are possible during this time. In this way, the strength of a brute force attack is basically nullified because modern hardware is capable of trying a vast range of possibilities in a very short time (which is no longer true after introducing the limit), and the system resources are not abused by having to check the validity of the latest attempt constantly.

SQL injection is a relatively simple attack as well, and vulnerabilities that allow for the attack are quite easy to avoid by some basic coding practices; however, SQL injections are still very successful types of attack. In a SQL injection, the attacker passes SQL (Structured Query Language) code to an online application through an input field or HTTP parameters to gain unauthorised access to a database. The idea is to get the application to run the sent code, which does something malicious. It can allow (read and write) access to unauthorised data, bypass authentication, or shut down/delete the database regardless of whether the database is on the same or a different server as the web page. To prevent SQL injections, any receiving data must be adequately sanitised. This means that the data must be checked for anything that should not be there (e.g. unexpected SQL code) or only use prepared statements, which basically limit what the database will accept as a valid query.

Cross-Site Scripting (XSS) is a client-side injection attack. It commonly targets scripts embedded in a page on the user's web browser. The vulnerabilities are caused by the internet security weaknesses of client-side scripting languages (i.e., HTML and JavaScript). XSS manipulates client-side scripts of a web application to achieve the malicious purposes of the attacker. The embedded script can then be executed every time a page is loaded or an associated event is triggered. XSS can be used to gather sensitive or personal information, redirect the user to other malicious sites, steal users' session cookies (which allows the attacker to impersonate the victim), alter the browser functionalities, deface a web page, or perform a DoS attack. XSS vulnerabilities are easy to find and fix by proper data validation across the website.

As its name suggests, Denial of Service (DoS) attacks are designed to make a service inaccessible. This is typically done by flooding the target with a large volume of traffic, making it slow and potentially crashing. While handling all the fake requests, the server's capacity to timely respond to legitimate requests is diminished or

completely halted. Distributed Denial-of-Service (DDoS) attack is an enhanced version of DoS. While DoS uses one attacking source, DDoS is an organised attack from multiple machines (often from a botnet). In addition to the possibility of generating larger amounts of traffic with a larger number of machines, DDoS is also useful for hiding the origin of the attack.

12 Protective Measures and Recommendations

Many of the protective measures organisations should take to prevent possible vulnerabilities, and attacks have already been mentioned in other chapters of this manual. Therefore, this is more or less a summary.

Ensure to educate and orientate your users, employees (teachers and administrative staff), and system administrators on the importance of sound and secure passwords, their role and responsibilities in recognising and preventing security threats and risks, and how to identify attacks and attempts at exploiting them. This is especially true for system administrators, who, in addition, are often not very experienced and have a lot to learn - configuring the operating system and LMS, managing users and their permissions, managing firewall rules, web server configuration, etc. All these factors are critical to security, so support their education and training to improve their skills.

Consider implementing multi-factor authentication. Use secure communication channels for all forms of communications/connections. Maintain your software so it is up to date and any newly discovered vulnerabilities are patched. Establish and regularly create new backups. Also, ensure the backups are working and that you can quickly reintroduce them into your live environment. Make sure to implement malware prevention mechanisms in your organisation.

Any larger organisation should define privacy policies, user security policies, and organisational structures and implement organisation-wide approaches for managing their information security risks, identify the data controls, define secure information sharing, etc.

13 Conclusion

In this manual, we have presented some of the most essential cybersecurity considerations to consider in the process of establishing and/or attending online learning. The content is primarily interesting for online learning providers, but useful information for students and teachers is included.

We have looked at the security issues that face users and administrators of Learning Management Systems (LMS) from the conceptual properties that must be achieved in order to establish a secure learning environment online, through threats that are present to, finally, some suggestions and recommendations on how effectively to protect the online learning environment.

We aimed to use this manual to connect with some other results produced in the Cyber F-IT project centred around privacy, information security management in higher education, and the configuration of the Moodle learning management system. Hopefully, this work will contribute to understanding how privacy and security are connected and give readers some background and understanding of what some of the security options in the configuration of Moodle are, why they are necessary, and how they help secure the system.

References

- Alwi, N. H. M., & Fan, I.-S. (2009). Information security management in E-learning. *International Conference for Internet Technology and Secured Transactions, ICITST 2009*. <https://doi.org/10.1109/ICITST.2009.5402507>
- Bandara, I., Ioraş, F., & Maher, K. (2014). *CYBER SECURITY CONCERNS IN E-LEARNING EDUCATION*.
- Buck, D. (n.d.). *CMS Security: How to Keep Your Website Safe*. Retrieved December 10, 2021, from <https://www.brandextract.com/Insights/Articles/CMS-Security-How-to-Keep-Your-Website-Safe/>
- Costinela-Luminita, D. (2011). Information security in E-learning Platforms. *Procedia - Social and Behavioral Sciences*, 15, 2689–2693. <https://doi.org/10.1016/J.SBSPRO.2011.04.171>
- Cybersecurity Risks in eLearning. (2021). *Virtru*. <https://www.virtu.com/blog/cyber-security-risks-e-learning/>
- Daniels, D. (2020, July 28). What Is SSL, TLS and HTTPS? <https://blog.gigamon.com/2019/09/06/gigamons-guide-to-communications-security-what-is-ssl-tls-and-https/>
- Furnell, S. M., & Karweni, T. (2001). Security issues in Online Distance Learning. *VINE*, 31(2), 28–35. <https://doi.org/10.1108/03055720010803998>

- Grassi, P., Newton, E., Fenton, J., Perlner, R., Regenscheid, A., Burr, W., Richer, J., Lefkowitz, N., Danker, J., Choong, Y.-Y., Greene, K., & Theofanos, M. (2017). NIST Special Publication 800-63B - Digital Identity Guidelines: Authentication and Lifecycle Management. In Special Publication (NIST SP) - 800-63B. <https://doi.org/10.6028/NIST.SP.800-63B>
- Hilmi, M. F., Pawanchik, S., Mustapha, Y., & Ali, H. M. (2013). Information Security Perspective of a Learning Management System. *International Journal of Knowledge Society Research*, 4(2), 9–18. <https://doi.org/10.4018/JKSR.2013040102>
- How to Secure Your Content Management System. (n.d.). Retrieved December 10, 2021, from <https://www.makeuseof.com/how-to-secure-your-content-management-system/>
- Malware | What is Malware & How to Stay Protected from Malware Attacks. (n.d.). Palo Alto Networks. Retrieved December 22, 2021, from <https://www.paloaltonetworks.com/cyberpedia/what-is-malware>
- Mening, R. (n.d.). 4 Security Tips To Help You Secure Your Online Learning Platform - eLearning Industry. Retrieved November 22, 2021, from <https://elearningindustry.com/secure-your-online-learning-platform-4-security-tips-help>
- Miguel, J., Caballé, S., & Prieto, J. (2013). Providing information security to MOOC: Towards effective student authentication. *Proceedings - 5th International Conference on Intelligent Networking and Collaborative Systems, INCoS 2013*, 289–292. <https://doi.org/10.1109/INCOS.2013.52>
- Nair, V. S. (2020). CMS Vulnerabilities: Why are CMS platforms common hacking targets? <https://beaglesecurity.com/blog/article/cms-vulnerabilities.html>
- Phishing Scams & Attacks - How to Protect Yourself. (n.d.). Kaspersky. Retrieved December 21, 2021, from <https://www.kaspersky.com/resource-center/preemptive-safety/phishing-prevention-tips>
- Rupaneliya, M. (n.d.). Data Security In Online Learning - eLearning Industry. Retrieved November 22, 2021, from <https://elearningindustry.com/understanding-data-security-in-online-learning>
- Rupareliya, M. (2020). Layman's Guide to Understanding Data Security In Online Learning. <https://elearningindustry.com/understanding-data-security-in-online-learning>
- Singh, B., & Kumar, B. (2020). Role of Cyber Security in E-Learning Education. *International Journal of Advanced Science and Technology*, 29(4s), 3172–3178. <http://sersc.org/journals/index.php/IJAST/article/view/22699>
- Stallings, W. (2023). *Cryptography and Network Security Principles and Practice*, 8ed, Global Edition, Pearson Education.
- Weippl, E. (2005). *Security in E-Learning* (Vol. 16). Springer-Verlag. <https://doi.org/10.1007/B136702>
- What is Malware? (n.d.). Cisco. Retrieved December 22, 2021, from <https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html>

PROTECTION OF PERSONAL DATA (GUIDELINES FOR EDUCATIONAL INSTITUTIONS AND STUDENTS)

ALJOŠA POLAJŽAR

University of Maribor, Faculty of Law, Maribor, Slovenia
aljosa.polajzar@um.si

Abstract The author discusses the protection of personal data by educational institutions in the context of the education process. The author introduces and explains the basic concepts in this area. It then goes on to discuss the fundamental principles of personal data protection that are relevant for any type of personal data processing, e.g. the data minimisation principle, according to which only data that are strictly necessary for the purpose of the processing may be processed. Compliance with these principles is essential for the lawful processing of personal data. Alongside the principles, each processing must be based on one of the lawful bases under the General Data Protection Regulation (GDPR). The obligations of the data controller (educational institutions) and the rights of data subjects (students) are also addressed. It is particularly important that the institution takes all necessary preventive and technological measures to ensure adequate processing. Particular diligence is also needed when dealing with special types of personal data. Finally, the consequences of possible breaches and the functioning of the supervisory authority, to which students can also turn in case of irregularities, are also highlighted.

Keywords:

personal data protection, General Data Protection Regulation (GDPR), data minimisation principle, consent of the data subject, obligations of the controller, rights of the data subject

1 Introduction and fundamental concepts¹

1.1 Introduction

In the area of e-learning, strict compliance with the rules related to the protection of personal data is essential. In online environments, individuals share a large amount of information about themselves, for example: age, email address, personal name, residential address, personal interests, etc. It is crucial that those who gain access to this information in the course of delivering education, treat this information in accordance with all the applicable rules (regarding the permissible handling, storage, processing, sharing, etc. of this data).

The European Union (EU) has adopted uniform rules on the protection of individuals with regard to the processing of personal data under a directly binding legal act: the General Data Protection Regulation (GDPR). The Regulation protects the fundamental rights and freedoms of individuals and, in particular, their right to the protection of personal data.² All educational institutions (and all their employees) operating in the EU must also comply with GDPR when processing personal data (e.g. of students). These rules comprehensively regulate the protection of personal data and apply uniformly regardless of the EU country (e.g. the same in Slovenia, France, Poland, Germany, etc.).³

It is true that, in the context of the GDPR, personal data is also protected (in each individual country) under the law(s) adopted by each individual EU country for this purpose. Similarly, educational (and other) institutions may also adopt various internal acts which may regulate in more detail the protection of personal data.

¹ This part of the manual was prepared by Aljoša Polajžar. The legal content is taken from the text of the provisions of the current General Data Protection Regulation (GDPR). Full name of the source: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), Official Journal L 119, available at URL: <https://eur-lex.europa.eu/legal-content/SI/TXT/?uri=CELEX%3A32016R0679> (accessed 16.6.2021).

Except where specifically indicated by a footnote, illustrations, possible practical examples and advice/guidance for educational institutions and students are provided by the author.

² Article 1, paragraph 2 of the General Data Protection Regulation (GDPR).

³ The Information Commissioner of the Republic of Slovenia also emphasises the importance of the GDPR for the protection of personal data in its guidelines – see: Information Commissioner, 2021, p. 5. For more on "regulation" as a generally binding EU legal act, see Borchardt, Klaus-Dieter, 2016, p. 92.

However, we would like to stress that all such acts (e.g. national laws, university regulations, etc.) must always be in line with the European regulation (GDPR). This means that they must not provide for a lower level of protection of the personal data of individuals (e.g. students) than under the GDPR, or deprive them of their rights guaranteed by the GDPR.⁴ Knowledge of the common, uniform European regulation is therefore the basis for the protection of personal data in the context of each EU country and the educational institutions operating in it. For this reason, the present Manual is also based exclusively on the uniform European regulation under the GDPR.

1.2 Fundamental concepts

At the outset, it is necessary to define the fundamental concepts related to the protection of personal data:

- **“personal data”** means any information relating to an identified or identifiable natural person (“data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.⁵

In other words, we are dealing with personal data when this information (data) is linked to a specific identifiable natural person. This information means “knowledge” about the person to whom it relates (e.g. a student's ID card number, place of birth, personal interests, email address, telephone number, IP address, etc.). In the context of our Manual, it is primarily students who will be the data subjects to whom personal data relates. Student's personal data must be adequately protected by the educational institutions.⁶

⁴ This follows from a fundamental general principle of EU law – the principle of primacy. See Borchardt, Klaus-Dieter, 2016, pp. 128-130.

⁵ Article 4, paragraph 1 of the General Data Protection Regulation (GDPR).

⁶ See also Information Commissioner, 2021, p. 7.

We should also point out that certain categories of particularly sensitive personal data relating to an individual (e.g. data revealing racial or ethnic origin, political opinions, biometric data, etc.) are particularly protected.⁷ The processing of such data is only possible under strict conditions (more on this in next chapters).

- **“processing of personal data”** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.⁸

Any handling (any activity) of information (personal data) in relation to a filing system of personal data, *or where automated processing occurs regardless of the existence of the filing system*, will constitute processing of that data.⁹ It is therefore particularly important to know when personal data may be processed or collected, recorded, disseminated, etc.

In practice, automated processing means that personal data are processed by automated means using a personal computer, mobile device, etc. Non-automated or *manual processing* of personal data will also be subject to the GDPR where the data forming part of a collection or intended to form part of a collection (e.g. a specially structured file). A filing system, on the other hand, is any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.¹⁰ Even documents in physical form may be arranged in such a way that they systematically collect a large amount of personal data that can be easily found in a consultation of that filing system.¹¹

⁷ European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 96.

⁸ Article 4, paragraph 2 of the General Data Protection Regulation (GDPR).

⁹ Information Commissioner, 2021, p. 7. See also Article 2, paragraph 1 of the General Data Protection Regulation (GDPR).

¹⁰ Article 4, paragraph 6 of the General Data Protection Regulation (GDPR).

¹¹ European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 100.

- **“controllers” of personal data:** in light of the legal rules, educational institutions (and their employees on their behalf) will collect or process personal data of their students. In this light, educational institutions will be considered as “controllers” of personal data. Educational institutions are “controllers” of personal data because they alone or jointly with other bodies determine the purposes and means of the processing.¹²

However, personal data processors will often also be involved in the processing of personal data. Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.¹³ For example, a processor will be a recruitment agency that processes personal data as a processor for other companies (which are data controllers of their employees' personal data). However, where that agency processes personal data of its own employees, it would be acting as a controller.¹⁴

- **“personal data breach”** in accordance with the GDPR, means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.¹⁵

All those involved in the educational process must take particular care to ensure that the above-mentioned breaches of personal data protection do not occur. For example, Article 82 of the GDPR provides that any individual who has suffered material or non-material damage as a result of an infringement of the GDPR has the right to obtain compensation from the controller or processor for the damage suffered.

¹² Article 4, paragraph 7 of the General Data Protection Regulation (GDPR). See also: Information Commissioner, 2021, p. 6.

¹³ Article 4, paragraph 8 of the General Data Protection Regulation (GDPR).

¹⁴ European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 107-108.

¹⁵ Article 4, paragraph 12 of the General Data Protection Regulation (GDPR).

2 Basic principles (rules) and grounds for the appropriate handling of personal data

2.1 Principles relating to the processing (handling) of personal data

In particular, personal data controllers (in our case, educational institutions and the employees within them who collect and process students' personal data) must take particular care to comply with the fundamental principles and rules of the GDPR. The most important fundamental principles common to all processing of personal data, which the study process providers should take into account when planning their activities, are:

- **“purpose limitation”** - personal data are collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes.¹⁶

In other words, this means that any collection or processing of personal data of students (e.g. collection of data on their foreign language skills, residential addresses, etc.) must clearly specify the explicit purpose of the data collection (e.g. the data is requested for the purpose of students' applications to participate in an international university project, for which excellent English language skills are required). This also means that the data collected may not be used for purposes other than those for which it was collected (e.g. the language proficiency data would be passed on to commercial providers of foreign language courses, etc.). The data may only be used (processed) for the purposes for which it was collected.¹⁷

- **“data minimisation principle”** - personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.¹⁸

¹⁶ Article 5, paragraph 1, point (b) of the General Data Protection Regulation (GDPR).

¹⁷ See also: European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 122-125.

¹⁸ Article 5, paragraph 1, point (c) of the General Data Protection Regulation (GDPR).

This means that before collecting or processing personal data, it is important to ask ourselves which personal data we absolutely need to fulfil our purpose. For example, if we are collecting applications from students to participate in an international research project, the necessary personal data could be previous work experience, foreign language skills, etc. As a general rule, however, it would not be necessary to collect and process students' data on their religion, financial situation, sexual orientation, etc., as these personal data are not relevant and necessary for the fulfilment of our purpose (selection of students to participate in an international research project). The data must be collected to the extent and in the manner that minimally interferes with the student's right to informational privacy.¹⁹

- **“storage limitation”** - personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.²⁰

This principle means that personal data controllers (educational institutions) must set appropriate time limits for the retention of students' personal data collected for a specific purpose. For example, there is no reason why personal data of students collected for the purpose of distance education (e.g. videos of students' assignment answers, etc.) should be kept for a longer period of time than is necessary for the assessment of that knowledge. The same applies to specific personal data provided by students in order to apply for participation in an international project. There is no reason why this data (of non-selected students) should be kept for several years after the selection procedure has been completed.²¹

- **“integrity and confidentiality”** - personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.²²

¹⁹ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 125-127.

²⁰ Article 5, paragraph 1, point (e) of the General Data Protection Regulation (GDPR).

²¹ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 129-130.

²² Article 5, paragraph 1, point (f) of the General Data Protection Regulation (GDPR).

In the light of this principle, it is essential that educational institutions choose technological solutions for the processing (storage, collection, etc.) of personal data that ensure adequate information security. Only in this way will the data collected from students (e.g. their email addresses, transaction account numbers, student ID numbers etc.) be protected against misuse by unauthorised third parties.²³

- **“lawfulness, fairness and transparency”** - personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject.²⁴

This principle will be furtherly described below in the Manual, as **“lawfulness”** refers to the choice of the appropriate legal basis for the processing (e.g. the processing is based on the student's informed consent; it is necessary for compliance with a legal or contractual obligation of the educational institution, etc.).²⁵

- **“transparency”** refers to the requirement to provide all necessary information to individuals (students) regarding the collection, processing of their personal data (e.g. who is collecting the data, who will process it, for what purposes, for how long, etc.) – see Chapter 3 of Part I of the Manual.²⁶

2.2 Grounds for processing (student consent and other grounds)

Any processing of personal data must, *inter alia*, respect all of the aforementioned fundamental principles and be based on one of the specified legal bases under Article 6 of the GDPR. The following legal bases will be particularly relevant in the context of distance education:

- **The processing is necessary for compliance with a legal obligation to which the controller is subject**²⁷

²³ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 131-134.

²⁴ Article 5, paragraph 1, point (a) of the General Data Protection Regulation (GDPR).

²⁵ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 117-118.

²⁶ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 118-122.

²⁷ Article 6, paragraph 1, points (c) and (e) of the General Data Protection Regulation (GDPR).

In certain cases, educational institutions are obliged to collect and process certain personal data of their students for the purpose of carrying out the study process. For example, for the purpose of carrying out education, it is necessary to keep a list of students registered for a particular exam (their personal names, registration ID number, sequential entry to the exam, etc.).²⁸

- **The processing is necessary for the performance of a contract to which the data subject is a party**²⁹

Educational institutions may also be linked to their students on a contractual basis (the student enters education on the basis of a contract). Again, educational institutions may process the personal data of students that are strictly necessary for the performance of this contract (e.g. the student's enrolment data, etc.).³⁰

- **Consent of the data subject**³¹

One of the most important legal bases for processing personal data is consent. Under the GDPR, "data subject consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.³²

It is important to note that the data subject has the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent prior to its withdrawal. The data subject shall be informed thereof before the consent is given. Consent shall be as easy to withdraw as to give.³³

²⁸ See also Information Commissioner, 2020.

²⁹ Article 6, paragraph 1, point (b) of the General Data Protection Regulation (GDPR).

³⁰ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, p. 151.

³¹ Article 6, paragraph 1, point (a) of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 142-151.

³² Article 4, paragraph 11 of the General Data Protection Regulation (GDPR).

³³ Article 7, paragraphs 2 and 3 of the General Data Protection Regulation (GDPR).

For example, students applying to participate in an international research project, etc., will normally be required to provide consent at the end of the form for the processing of the personal data provided for that specific purpose. In the present case, educational institutions will have to carefully follow all the above rules on consent and ensure that the student's consent is free, explicit and informed. The student should also be made aware of the possibility to withdraw consent afterwards.

2.3 Processing of special categories of personal data

We would also like to highlight Article 9 of the GDPR, which, in the light of the basic principles already outlined, lays down specific conditions for the processing of special types of (particularly sensitive) personal data³⁴, which may also be encountered in the course of the provision of education. The Article provides that the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.³⁵

However, this rule does not apply if one of the specified exceptions under Article 9 of the GDPR applies. In the context of education, the relevant exception is under point (a), which provides that the prohibition does not apply where the data subject has given his or her explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provides that the data subject may not derogate from that prohibition. Furthermore, the relevant ground under point (c) may be that the processing is necessary to protect the vital interests of the data subject or of another individual where the data subject is physically or legally incapable of giving consent. Also relevant is the exception under point (f) that processing is necessary for the establishment, exercise or defence of legal claims or whenever the courts are acting in their judicial capacity. The latter could be relevant in the case of a specific legal dispute between a student and an educational institution. Furthermore, in times of health crises the ground under point (i) may be relevant: processing is necessary for reasons of public interest in the

³⁴ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 96, 159-165.

³⁵ Article 9, paragraph 1 of the General Data Protection Regulation (GDPR).

field of public health, such as protection against serious cross-border health risks on the basis of Union law or the law of a Member State which provides for appropriate and specific measures to safeguard the rights and freedoms of the data subject. Finally, it is worth mentioning the ground under point (j), which may be relevant in the context of the performance of research: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes pursuant to Article 89(1) of the GDPR on the basis of Union or Member State law which is proportionate to the aim pursued, respects the essence of the right to data protection and ensures appropriate and specific measures to safeguard the data subject's fundamental rights and interests.³⁶

2.4 Conclusion

The conditions that the processing is necessary for the performance of a contract (e.g. an education contract) or necessary for compliance with a legal obligation of the controller (e.g. the provision of education under a specific programme) may be particularly relevant at the time of distance education in the light of the epidemiological measures related to COVID-19. In such cases, the collection and processing of personal data through online classrooms may be necessary for conducting the educational process in certain cases (e.g. where it is not possible to conduct the examination in person, it may be necessary to have a video link between the professor and the student, etc.).³⁷

However, we would like to stress that the basic principles of the processing of personal data (the principle of data minimisation, the principle of transparency, purpose limitation and storage limitation) should be respected or complied with in all cases by the providers of the educational process.

Therefore, as a general guideline for personal data controllers (educational institutions and their employees), it may serve to ask: Is there an adequate basis for collecting or processing students' personal data? Does the collection or processing respect the principles of data minimisation (only the data necessary for the purpose of processing are processed) and transparency (students are provided with all

³⁶ Article 9, paragraph 2 of the General Data Protection Regulation (GDPR).

³⁷ See, for example, its opinion on "Distance education and the protection of personal data" (Information Commissioner, 2020).

necessary information concerning the processing of their data)? Will the processing of personal data in any case be carried out in an appropriate technical and organisational manner to ensure its security (including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)? In particular, when choosing technological solutions, it is important to bear in mind whether our legitimate purpose/objective (because of which we are collecting and processing personal data) could be achieved in a way that would be less intrusive into the students' right to privacy.³⁸

3 Rights of individuals (students) and obligations of controllers (educational institutions)³⁹

Data subjects (e.g. students enrolled in education) also have certain important rights relating to their personal data.

3.1 Rights exercised directly with the educational institution (data controller of students' personal data)

Right of access and information: the data subject has the right to obtain from the controller confirmation as to whether personal data concerning him or her are being processed and, where this is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

³⁸ On the importance of respecting the fundamental rules/principles of personal data protection, see also: Information Commissioner, 2021, pp. 8-9.

³⁹ This chapter is based on the provisions of the GDPR. As an example of the information provided by the University of Maribor regarding the protection of personal data, see for basic information: <https://www.um.si/univerza/varstvo-osebni-podatkov/Strani/default.aspx> (accessed 1.6.2021) and for information regarding the rights of the individual: <https://www.um.si/univerza/varstvo-osebni-podatkov/Strani/Pravice-posameznika.aspx> (accessed 16.6.2021). For more information on individuals' rights, see also the Information Commissioner's Guidelines (2021), pp. 10-17.

- where possible, the envisaged period of retention of the personal data or, if this is not possible, the criteria to be used to determine that period;
- the existence of a right to obtain from the controller the rectification or erasure of personal data or the restriction of the processing of personal data concerning the data subject, or the existence of a right to object to such processing;
- the right to lodge a complaint with the supervisory authority;
- where the personal data are not collected from the data subject, any available information concerning their source;
- the existence of automated decision-making, including profiling, and, at least in such cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.⁴⁰

In practice, this means that it is important that the collection or processing of personal data is transparent (individuals must be informed in advance and have the right to request relevant information).

Right to rectification: the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.⁴¹

Right to erasure ("right to be forgotten")⁴²: the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;

⁴⁰ Article 15, paragraph 1 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 216-219.

⁴¹ Article 16 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 219-221.

⁴² See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 221-227.

- the data subject withdraws the consent on the basis of which the processing is carried out and where there is no other legal basis for the processing;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data must be erased in order to comply with a legal obligation under EU or Member State law to which the controller is subject.⁴³

However, an individual (e.g. a student) does not have the right to have his/her personal data forgotten or deleted if processing is necessary:

- to exercise the right to freedom of expression and information;
- for compliance with a legal obligation to process under EU law or the law of a Member State to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the field of public health;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- to assert, exercise or defend legal claims.⁴⁴

Right to restriction of processing:⁴⁵ The data subject has the right to obtain from the controller the restriction of processing where one of the following applies:

- the data subject contests the accuracy of the data for a period which allows the controller to verify the accuracy of the personal data;
- the processing is unlawful and the data subject objects to the erasure of the personal data and requests instead the restriction of their use;
- the controller no longer needs the personal data for the purposes of the processing, but the data subject needs them for the establishment, exercise or defence of legal claims;

⁴³ Article 17, paragraph 1 of the General Data Protection Regulation (GDPR).

⁴⁴ Article 17, paragraph 3 of the General Data Protection Regulation (GDPR).

⁴⁵ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 227-228.

- the data subject has raised an objection to the processing, pending verification whether the legitimate grounds of the controller override those of the data subject.⁴⁶

Where the processing of personal data has been restricted in accordance with these rules, such personal data (with the exception of their storage) shall be processed only with the consent of the data subject, or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person, or for important reasons in public interest of the EU or of a Member State.⁴⁷

Right to object:⁴⁸ The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time, to processing of personal data concerning him or her based on point (e)⁴⁹ or (f)⁵⁰ of Article 6(1) of the GDPR, including profiling based on these provisions. The controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims.⁵¹ The data subject shall be explicitly informed of the right to object at the latest at the time of the first communication with him or her and shall be presented with this right clearly and separately from any other information.⁵²

In practice, the student thus has the possibility to request the erasure, rectification or restriction of the processing of personal data that he or she has provided to the educational institution (provided that the conditions set out above are fulfilled). The student may have an interest in carrying out these actions in different situations. For example, if he or she so wishes, he or she may request the erasure of the personal data provided for the purpose of applying to participate in a research project for which he or she has not been selected. Similarly, if his/her personal data are

⁴⁶ Article 18, paragraph 1 of the General Data Protection Regulation (GDPR).

⁴⁷ Article 18, paragraph 2 of the General Data Protection Regulation (GDPR).

⁴⁸ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 229-233.

⁴⁹ The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

⁵⁰ The processing is necessary for the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

⁵¹ Article 21, paragraph 1 of the General Data Protection Regulation (GDPR).

⁵² Article 21, paragraph 4 of the General Data Protection Regulation (GDPR).

incorrectly indicated in the publications on the website of the educational institution (e.g. an error in the personal name of a student who participated in a particular project), he/she may request that this information to be corrected.

3.2 Rights that students can exercise with the external national supervisory authority

Right to lodge a complaint with a supervisory authority: every data subject has the right to lodge a complaint with a supervisory authority, in particular in the EU country where he or she is habitually resident, where he or she has his or her place of work or where the alleged infringement has occurred – if he or she considers that processing of personal data concerning him or her infringes GDPR provisions.⁵³ The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy.⁵⁴

Supervisory authorities: each EU country shall provide one or more independent public authorities competent to monitor the application of this Regulation in order to protect the fundamental rights and freedoms of individuals with regard to processing and to facilitate the free flow of personal data within the EU.⁵⁵

For individuals (students), the supervisory authority can be important in practice, as each supervisory authority has the following tasks in its territory:

- promote public awareness and understanding of the risks, rules, safeguards and rights related to processing;
- promote awareness among controllers and processors of their obligations under GDPR;
- provide information to any data subject, upon request, on the exercise of his or her rights under the GDPR and, to that end, cooperate, where appropriate, with supervisory authorities in other Member States;

⁵³ Article 77, paragraph 1 of the General Data Protection Regulation (GDPR).

⁵⁴ Article 77, paragraph 2 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 237-238.

⁵⁵ Article 51, paragraph 1 of the General Data Protection Regulation (GDPR).

- deal with complaints lodged by the data subject;
- cooperate with other supervisory authorities, including by exchanging information, and provide mutual assistance to ensure consistency in the application and enforcement of GDPR.⁵⁶

The performance of these tasks by each supervisory authority is free of charge for the data subject.⁵⁷

It follows from the above that students may also directly contact an independent external state authority for the protection of personal data (in Slovenia, the Information Commissioner) in the event of alleged irregularities in the handling of their personal data. Nevertheless, it would be appropriate (in line with the spirit of the relationship between the students and the educational institution) that in case of alleged irregularities, the student should first contact the educational institution, which will check whether everything is in line with the rules and rectify any irregularities. If the individual (e.g. the student) is not satisfied with the solution, he/she can, of course, also contact the aforementioned national authority. We would also like to point out that the authority will help the individual (student) free of charge (the question, complaint, letter, etc. can also be sent to the authority by e-mail, telephone, etc.). There are no costs involved, as is the case, for example, with court proceedings.

It is also worth noting that in the case of cross-border studies (for example, if students are studying remotely (or coming) from a country other than the country where the educational institution is based), they have the right to contact the supervisory authority in their home country or in the country where the educational institution is based. As mentioned above, the supervisory authorities of the different countries have the duty to cooperate with each other, which will help to resolve the issue at hand.

⁵⁶ Articles 57 and 58 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 194-199.

⁵⁷ Article 57, paragraph 3 of the General Data Protection Regulation (GDPR).

3.3 Obligations of controllers (educational institutions) and processors of personal data

The GDPR further **specifies a number of obligations for controllers of personal data** (in our case, educational institutions). Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.⁵⁸ Where proportionate to the processing activities, the measures taken pursuant to those obligations shall include the implementation by the controller of appropriate data protection policies.⁵⁹

Furthermore, the **concept of personal data protection by design and by default is also important**.⁶⁰ The GDPR provides that, taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.⁶¹ It further provides that the controller shall implement appropriate technical and organisational measures to ensure that, by default, only the personal data necessary for each specific purpose of processing are processed. This obligation applies to the amount of personal data collected, the scope of their processing, their retention period and their accessibility. In particular, such measures shall ensure that personal data are not automatically accessible to an

⁵⁸ Article 24, paragraph 1 of the General Data Protection Regulation (GDPR).

⁵⁹ Article 24, paragraph 2 of the General Data Protection Regulation (GDPR).

⁶⁰ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 183-185.

⁶¹ Article 25, paragraph 1 of the General Data Protection Regulation (GDPR).

indeterminate number of individuals without the intervention of the individual concerned.⁶²

The GDPR also imposes an obligation to keep records of **processing activities**.⁶³ Each controller and the controller's representative, where one exists, shall keep a record of the processing activities of personal data under its responsibility. This record shall contain the following information:

- (a) the name and contact details of the controller and, where they exist, of the joint controller, the controller's representative and the data protection officer;
- (b) the purposes of the processing;
- (c) a description of the categories of data subjects and types of personal data;
- (d) the categories of users to whom personal data have been or will be disclosed, including users in third countries or international organisations;
- (e) where applicable, information on transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation;
- (f) where possible, the time limits foreseen for the deletion of different types of data;
- (g) where possible, a general description of the technical and organisational safety measures.⁶⁴

Article 32 of the GDPR also places an important emphasis on the **security of processing**.⁶⁵ The provision provides that, taking into account the latest technological developments and the costs of implementation, as well as the nature, scope, circumstances and purposes of the processing, and the risks to the rights and freedoms of natural persons, which vary in likelihood and severity, the controller and the processor shall ensure an appropriate level of security in relation to the risk, by implementing appropriate technical and organisational measures, including, but not limited to, the following measures, as appropriate:

- (a) pseudonymisation and encryption of personal data;

⁶² Article 25, paragraph 2 of the General Data Protection Regulation (GDPR).

⁶³ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 178-179.

⁶⁴ Article 30, paragraph 1 of the General Data Protection Regulation (GDPR).

⁶⁵ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 165-169.

- (b) the ability to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.⁶⁶

Furthermore, the GDPR provides that the determination of the appropriate level of security shall take into account, in particular, the risks posed by the processing, in particular due to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.⁶⁷

The controller and the processor shall also ensure that any natural person acting under the authority of the controller or the processor who has access to personal data may not process it without the controller's instructions, unless required to do so by EU or Member State law.⁶⁸

Data controllers also have a specific obligation to **notify the supervisory** authority of a personal data breach. In the event of a personal data breach, the controller shall notify the competent supervisory authority without undue delay and preferably not later than 72 hours after becoming aware of the breach, unless the personal data breach is unlikely to jeopardise the rights and freedoms of natural persons. Where notification to the supervisory authority is not given within 72 hours, it shall be accompanied by a statement of the reasons for the delay.⁶⁹

In accordance with the GDPR, the notification must contain at least:

- (a) a description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the types and approximate number of personal data records concerned;

⁶⁶ Article 32, paragraph 1 of the General Data Protection Regulation (GDPR).

⁶⁷ Article 32, paragraph 2 of the General Data Protection Regulation (GDPR).

⁶⁸ Article 32, paragraph 4 of the General Data Protection Regulation (GDPR).

⁶⁹ Article 33, paragraph 1 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 171-173.

- (b) a communication of the name and contact details of the data protection officer or other contact point from whom more information can be obtained;
- (c) a description of the likely consequences of the personal data breach;
- (d) a description of the measures taken or proposed to be taken by the controller to address the personal data breach, as well as measures to mitigate any adverse effects of the breach, if appropriate.⁷⁰

The controller has an obligation to document any personal data breach, including the facts relating to the personal data breach, its effects and the corrective measures taken.⁷¹

Data protection impact assessment and prior consultation are two important obligations of the data controller (educational institution). A data **protection impact assessment (DPIA)** shall be carried out where it is possible that the type of processing, in particular through the use of new technologies, taking into account the nature, scope, context and purposes of the processing, may result in a high risk to the rights and freedoms of natural persons. In such cases, the controller shall therefore carry out an assessment of the impact of the envisaged processing operations on the protection of personal data before processing. A single assessment may address a set of similar processing operations presenting similar high risks.⁷² The GDPR provides that when carrying out a data protection impact assessment, the controller shall seek the opinion of the Data Protection Officer, where appointed.⁷³

For our case, it is relevant that a data protection impact assessment is required in particular in the case of:

- (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

⁷⁰ Article 33, paragraph 3 of the General Data Protection Regulation (GDPR).

⁷¹ Article 33, paragraph 5 of the General Data Protection Regulation (GDPR).

⁷² Article 35, paragraph 1 of the General Data Protection Regulation (GDPR).

⁷³ Article 35, paragraph 2 of the General Data Protection Regulation (GDPR).

- (b) large-scale processing of special categories of data within the meaning of Article 9 of the GDPR.⁷⁴

The GDPR further specifies that the data protection impact assessment shall provide at least:

- (a) a systematic description of the envisaged processing operations and the purposes of the processing and, where applicable, the legitimate interests pursued by the controller;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to their purpose;
- (c) an assessment of the risks to the rights and freedoms of data subjects; and
- (d) measures to address risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.⁷⁵

Depending on each individual case and the technology deployed, the data protection impact assessment may be crucial for the lawful functioning of educational institutions. Especially in light of the large amounts of student's personal data that the educational institutions are processing.

Furthermore, the GDPR foresees an **obligation of prior consultation**.⁷⁶ The controller shall consult the supervisory authority before processing where it is apparent – from the data protection impact assessment referred to in Article 35 of the GDPR – that the processing would result in a high risk if the controller did not take measures to mitigate the risk.⁷⁷ Where the supervisory authority considers that the envisaged processing would infringe the GDPR, in particular where the controller has not adequately identified or mitigated the risks, the supervisory authority shall, within a period of up to eight weeks after receipt of the request for consultation, advise the controller in writing. This period may be extended by a further six weeks, taking into account the complexity of the envisaged processing.

⁷⁴ Article 35, paragraph 3 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 179-181.

⁷⁵ Article 35, paragraph 7 of the General Data Protection Regulation (GDPR).

⁷⁶ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 179-181.

⁷⁷ Article 36, paragraph 1 of the General Data Protection Regulation (GDPR).

The supervisory authority shall inform the controller and, where necessary, the processor of any such extension within one month of receipt of the request for consultation, together with the reasons for the delay. That period may be suspended until the supervisory authority has obtained the information it requested for the purposes of the consultation.⁷⁸

The Data Protection Officer also plays an important role in ensuring the protection of personal data within the organisation.⁷⁹ The controller and the processor shall appoint a data protection officer whenever processing is carried out by a public authority or body. The data protection officer may be a member of the controller's or processor's staff or may perform the tasks on the basis of a service contract. The controller or processor must publish the contact details of the data protection officer and communicate them to the supervisory authority.⁸⁰

The Data Protection Officer also has a specific position. The controller and the processor shall ensure that the data protection officer is involved in an appropriate and timely manner in all matters relating to the protection of personal data.⁸¹ The controller and the processor shall also assist the data protection officer in the performance of these tasks by providing the means necessary for the performance of the tasks and access to personal data and processing operations, and by maintaining the expertise of the data protection officer.⁸² The controller and the processor shall ensure that the data protection officer does not receive any instructions in the performance of his tasks. The data protection officer shall not be dismissed or penalised for the performance of his or her tasks. The DPO shall report directly to the highest management level of the controller or processor.⁸³

Data subjects may contact the Data Protection Officer in relation to any matter concerning the processing of their personal data and the exercise of their rights under the GDPR.⁸⁴ The Data Protection Officer shall be bound by the obligation

⁷⁸ Article 36, paragraph 2 of the General Data Protection Regulation (GDPR).

⁷⁹ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 175-178.

⁸⁰ Article 37, paragraphs 1, 6 and 7 of the General Data Protection Regulation (GDPR).

⁸¹ Article 38, paragraph 1 of the General Data Protection Regulation (GDPR).

⁸² Article 38, paragraph 2 of the General Data Protection Regulation (GDPR).

⁸³ Article 38, paragraph 3 of the General Data Protection Regulation (GDPR).

⁸⁴ Article 38, paragraph 4 of the General Data Protection Regulation (GDPR).

of secrecy or confidentiality in the performance of his or her duties under Union or Member State law.⁸⁵

Furthermore, the Data Protection Officer has at least the following tasks:

- (a) informing and advising the controller or processor and the employees carrying out the processing of their obligations under the GDPR and other provisions of Union or Member State law on data protection;
- (b) monitoring compliance with the GDPR, other provisions of Union or Member State law on data protection and the controller's or processor's policies on the protection of personal data, including the assignment of tasks, awareness-raising and training of staff involved in processing operations and related audits;
- (c) advising, where requested, on the data protection impact assessment and monitoring its implementation;
- (d) cooperation with the supervisory authority;
- (e) acting as a contact point for the supervisory authority on issues relating to processing, including prior consultation, and, where appropriate, consultation on any other matter.⁸⁶

It can be concluded that all these obligations of the controller (the educational institution) contribute to a systemically higher protection of students' personal data within the organisation. Both the prior data protection impact assessment procedures when implementing new systems and the appointment of a Data Protection Officer play an important role. The latter is an important point of contact both for the supervisory authorities monitoring the compliance of the educational institution's practices with the GDPR and for the individuals (students) whose data are processed.

3.4 Consequences of personal data breaches

Compliance with the provisions of the GDPR is important not only because of the importance of protecting individuals' rights, but also because of the potential consequences that breaches may bring.

⁸⁵ Article 38, paragraph 5 of the General Data Protection Regulation (GDPR).

⁸⁶ Article 39, paragraph 1 of the General Data Protection Regulation (GDPR).

As already mentioned, the GDPR provides that any individual who has suffered material or non-material damage as a result of an infringement of GDPR provisions has the right to obtain compensation from the controller or processor for the damage suffered.⁸⁷ Any controller involved in processing shall be liable for the damage caused by processing in breach of the GDPR. The processor shall be liable for the damage caused by the processing only where it has failed to comply with the obligations under GDPR specifically addressed to processors or where it has exceeded or acted contrary to the lawful instructions of the controller.⁸⁸ The controller or processor shall be exempted from liability if they prove that they are in no way responsible for the event giving rise to the damage.⁸⁹

Another important form of liability is the liability to commit an offence or to pay a penalty (administrative fine) for breaches of the rules on the protection of personal data.⁹⁰ As a general rule, the fines imposed should be proportionate, effective and dissuasive for the offenders.⁹¹

In deciding whether to impose an administrative fine and the amount of the administrative fine in each case, due account shall be taken of the following:

- (a) the nature, gravity and duration of the breach, taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected by the breach and the level of damage suffered by them;
- (b) whether the infringement is intentional or due to negligence;
- (c) any measures taken by the controller or processor to mitigate the damage suffered by data subjects;
- (d) the degree of responsibility of the controller or processor, taking into account the technical and organisational measures adopted by the controller or processor in accordance with the GDPR;
- (e) any relevant previous infringements by the controller or processor;

⁸⁷ Article 80, paragraph 1 of the General Data Protection Regulation (GDPR).

⁸⁸ Article 80, paragraph 2 of the General Data Protection Regulation (GDPR).

⁸⁹ Article 80, paragraph 3 of the General Data Protection Regulation (GDPR). See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 246-247.

⁹⁰ See also European Union Agency for Fundamental Rights and Council of Europe, 2018, pp. 247-248.

⁹¹ Article 83, paragraph 1 of the General Data Protection Regulation (GDPR).

- (f) the degree of cooperation with the supervisory authority in remedying the breach and mitigating any adverse effects of the breach;
- (g) the types of personal data concerned by the breach,
- (h) how the supervisory authority became aware of the infringement, in particular if and to what extent the controller or processor notified the infringement to the supervisory authority;
- (i) where warning measures of the supervisory authority under other provisions of the GDPR have been previously ordered against the controller or processor concerned in relation to the same subject matter, compliance with those measures;
- (j) commitment to approved codes of conduct or approved validation mechanisms; and
- (k) any other aggravating or mitigating factors relating to the circumstances of the case, such as financial benefits gained or losses avoided resulting directly or indirectly from the infringement.⁹²

In addition, GDPR rules provide that if a controller or processor intentionally or negligently infringes several provisions of the GDPR in the same or a related processing operation, the total amount of the administrative fine shall not exceed the amount set for the most serious infringement.⁹³

We would also like to highlight the level of administrative fines that can be imposed on the controller or processor of personal data. Infringements of the following provisions may be subject to administrative fines of up to EUR 10,000,000 or, in the case of a company, up to 2% of the total worldwide annual turnover in the preceding financial year, whichever is higher: obligations of the controller and the processor (e.g. to provide for the protection of personal data by default, to keep records of processing activities, to consult and report to the supervisory authority, to provide for a prior impact device for the protection of personal data, etc.) – Articles 35 to 39 of the GDPR.⁹⁴

⁹² Article 83, paragraph 2 of the General Data Protection Regulation (GDPR).

⁹³ Article 83, paragraph 3 of the General Data Protection Regulation (GDPR).

⁹⁴ Article 83, paragraph 4 of the General Data Protection Regulation (GDPR).

However, even higher fines – up to EUR 20,000,000 or, in the case of a company, up to 4% of the total worldwide annual turnover in the previous financial year, whichever is higher – can be imposed for breaches of the fundamental rules of processing, which we have also presented in this article: the basic principles of processing, including consent, breach of the rights of the data subject, etc. These are in particular the fundamental rules that we have presented in our article.⁹⁵

4 Conclusion

Respect for the protection of personal data is one of the most important issues in the provision of (online) education. In the course of their work, educational institutions manage a large amount of students' personal data. To this end, the GDPR comprehensively regulates the rules for the appropriate handling of personal data. These EU-wide uniform rules must be respected by all educational institutions operating in the EU.

As a starting point, it is important to start from the basic concepts (personal data, processing of personal data) that condition the application of the GDPR rules. Of particular importance are the initial fundamental principles relating to the processing of personal data (purpose limitation, data minimisation, storage limitation, integrity and confidentiality, etc.). Thus, personal data may only be processed for a specific legitimate purpose; to the extent necessary for the fulfilment of these purposes etc. The processing must also be based on one of the lawful legal bases under Article 6 GDPR. In this respect it is particularly important that the student's consent complies with all the standards under the GDPR. In the context of the provision of education, the ground that the processing is necessary for compliance with a legal obligation to which the controller is subject may also be relevant. Particular diligence must also be taken into account when dealing with special types of (sensitive) personal data for which there are specific rules for processing.

Therefore, as a general guideline for personal data controllers (educational institutions and their employees), it may serve to ask: Is there an adequate basis for collecting or processing students' personal data? Does the collection or processing respect the principles of data minimisation (only the data necessary for the purpose

⁹⁵ Article 83, paragraph 5 of the General Data Protection Regulation (GDPR).

of processing are processed) and transparency (students are provided with all the necessary information concerning the processing of their data)? Will the processing of personal data in any case be carried out in an appropriate technical and organisational manner to ensure its security (including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage)? In particular, when choosing technological solutions, it is important to bear in mind whether our legitimate purpose/objective (because of which we are collecting and processing personal data) could be achieved in a way that would be less intrusive into the students' right to privacy.

Furthermore, the GDPR regulates a number of obligations of the controller (educational institutions) and the rights of data subjects (students, employees). The data subject can exercise directly with the educational institution the right of access to information concerning the processing of personal data, the right to rectification of personal data, the right to erasure (right to be forgotten), the right to restriction of processing and the right to object. In the event of a breach, the individual may also have recourse to an independent external supervisory authority, to which he or she may lodge a complaint.

In this context, controllers (educational institutions) also have important obligations to ensure systemic security and lawful processing of personal data. Thus, when implementing various technological solutions in the educational process, they must take into account the concept of protection of personal data by design and by default, the consistent keeping of records of processing activities where necessary and the security of processing. In certain cases, it is mandatory or advisable to carry out a data protection impact assessment analysing the level of risk to the protection of personal data. A specially designated data protection officer also plays an important role for the protection of personal data within the organisation (educational institution).

In the event of irregularities, it should be stressed that students can contact the educational institution or the competent national supervisory authority. Employees or the educational institution must take particular care in handling personal data, as any breaches may result in liability for damages, and employment or criminal offences.

Students and employees can always find out more about personal data protection on the websites of the educational institution or national data protection authority. Another possibility is to contact the data protection officer within the organisation or the supervisory authority directly.

Notes

The author originally prepared the Manual in the Slovenian language. Versions in other languages represent a translation of the author's version written in Slovenian.

References

- Borchardt, Klaus-Dieter, *Fundamentals of European Union Law*, 2016, URL: http://publications.europa.eu/resource/cellar/5d4f8cde-de25-11e7-a506-01aa75ed71a1.0008.03/DOC_1 (accessed 26.6.2021).
- European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European data protection law: 2018 edition*, Publications Office of the European Union, Luxembourg 2018, URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf (accessed 26.6.2021), pp. 122-125.
- Information Commissioner, 2021 (Guide to personal data protection for individuals), URL: https://www.ip-rs.si/fileadmin/user_upload/Pdf/vodniki/Vodnik_po_varstvu_osebnih_podatkov_za_posameznike.pdf (accessed 26.6.2021).
- Information Commissioner, 2020, Opinion: 'Distance education and personal data protection', Date: 06.04.2020, Number: 07120-1/2020/274, URL: <https://www.ip-rs.si/mnenjajgdpr/6048a487a0e79> (accessed 26.6.2021).
- University of Maribor, *Personal Data Protection*, URL: <https://www.um.si/univerza/varstvo-osebnih-podatkov/Strani/default.aspx> (accessed 26.6.2021).
- University of Maribor, *Individual Rights*, URL: <https://www.um.si/univerza/varstvo-osebnih-podatkov/Strani/Pravice-posameznika.aspx> (accessed 26.6.2021).
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), Official Journal L 119, available at URL: <https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32016R0679> (accessed 26.6.2021).

LABOUR LAW AND CYBERSECURITY IN HIGHER EDUCATION

KLEMEN DRNOVŠEK

University of Maribor, Faculty of Law, Maribor, Slovenia
klemen.drnovsek@um.si

Abstract In this chapter, labour law aspects of cybersecurity in the higher education sector are presented. Labour law regulations set the rights and obligations of employees both in the case of typical and atypical labour relations. The worker can also work remotely (teleworking) or in home office (homeworking), respectively, whilst in this case, they must respect legislative provisions and instructions by their employer. Internet development and digitalisation essentially influenced the field of labour law. Due to the consequences of the pandemic disease COVID-19, drastic changes also appeared in the field of higher education practically overnight. The use of e-mail, data clouds, e-learning environments, video conference ways of conducting the study process, the examination and other internet activities of performance of study programmes represent different risks that must be tackled by higher education institutions. Aiming to lower security risks, educational institutions must constantly recognise these and train their employees in proper ways to provide for cybersecurity.

Keywords:
labour law;
employment law,
cybersecurity,
higher education,
COVID-19,
security policy,
diligence,
liability,
mitigation of risks

1 General

Labour can be performed on the basis of various legal bases, whereby the choice of the appropriate legal basis depends primarily on the nature of the work that the individual performs. In higher education, labour is done by scholars, higher education employees, researchers and students, who perform pedagogical and research labour, as well as by administrators performing technical, administrative, professional and other tasks. Despite the very varying nature of work of people employed in higher education institutions, practically all do their labour based on an employment contract. Due to specific work, the labour of scholars steps out. However, relations towards higher education institution still remains such that by performing their labour scholars meet the basic elements of a labour relation. A labour relation exists, when an individual does labour in a way that he or she is included in an organised labour process and does labour for payment, personally and without interruption, in line with instructions and under supervision by the employer, in our case – the higher education institution. Only exceptionally, the base of labour may be another contract of civil law (e.g., copyright agreement) or another legal base appearing especially in cases of short-term and occasional labour, for example when a certain lecturer conducts only an individual lecture or module at some higher education institution and obtains payment for that.

For all employees who have concluded employment contracts, or whose nature of work meets the elements of an employment relationship (Darja Senčur Peček & Franca, 2019: 114-132), special rights and obligations apply, which are grouped under the term "Labour Law". On the one hand, there are rules relating to the individual relationship between the employee and the employer (Employment Law). These include, in particular rules on the conclusion of employment contracts, their termination, remuneration, distribution of working time, breaks and rest periods, annual leave, protection of certain categories of workers, liability of the employee and the employer, etc. On the other hand, Labour Law consists of rules that regulate the relationship between workers' associations (unions) and employers or employers' associations (Collective Labour Law). In this case, these are autonomous rules that are not set by the legislator but are the result of negotiations and mutual agreement between the various stakeholders in the employment relationship. Consequently, the rules of labour law are regulated in various heteronomous and autonomous legal

acts. The basic source of any employment relationship is the employment contract, which must not contradict cogent regulations.

At the European Union level, a set of rules and arrangements have been adopted governing various areas of labour law and must be considered in the national laws of the Member States¹. Among the autonomous sources, in addition to collective agreements at various levels (at the level of the employer – e.g., Harvard University & Harvard Union of Clerical and Technical Workers Agreement², at the branch level - e.g., Collective Labour Agreement for Dutch Universities³, and general (unilateral) acts of the employer by which the employer regulates the organization of work - e.g., Rules on the protection of personal and confidential data at the University of Ljubljana⁴).

Labour law is a relatively young industry that began to develop in the early 19th century during the Industrial Revolution. The purpose of the first acts was in particular to improve working conditions (e.g., adequate ventilation of premises), to limit working hours (e.g., a maximum of 10 hours per day), to set restrictions on the work of children and women, etc. Over time, the rules of labour law have spread to virtually every area of our lives. It is characteristic of a classic employment relationship that the employee performs work on the employer's premises, whereby the employer must provide appropriate working conditions, working means, providing protective equipment and a safe and healthy working environment. Initially, the requirement to ensure a safe and healthy environment was mainly related to material circumstances (e.g., machinery, hazardous substances, etc.), but today the emphasis is on intangible assets such as online security, mental health, etc.

¹ See <https://eur-lex.europa.eu/summary/chapter/1717.html>.

² Harvard University & Harvard Union of Clerical and Technical Workers Agreement, available at <https://hr.harvard.edu/union-contracts>.

³ Collective Labour Agreement for Dutch Universities, available at: https://www.vsnunl/en_GB/cao-universiteiten.html

⁴ Rules on the protection of personal and confidential data at the University of Ljubljana, available at: https://www.uni-lj.si/university/organization_legal_framework_and_reports/statutes_of_ul_and_regulations/

2 Teleworking

There are several types of employment relationships. A typical employment relationship is based on a full-time employment contract, which depends on national law and is between 35 and 40 hours per week. A typical employment contract is concluded for an indefinite period (it can only be terminated in the case of specific conditions), and the work is performed at the employer's premises. There are several types of atypical employment contracts, e.g., part-time contracts, fixed-term contracts, and atypical employment contracts also include employment contracts for homeworking or teleworking.

Although cybersecurity issues occur in virtually all employment relationships, they are most common in the case of teleworking, so the focus of this paper will be on this atypical form of employment.

In order to establish a general framework for teleworking and to ensure greater protection for employees, the European Trade Union Confederation (ETUC), the Union of Industrial and Employers' Confederations of Europe / the European Union of Crafts and Small and Medium-Sized Enterprises (UNICE / UEAPME), and the Center of Enterprises with Public Participation (ECPE) signed Framework Agreement on Telework (July 2002)⁵; The agreement defined telework as a form of organizing and/or performing work, using information technology, in the context of an employment relationship, where work, which could also be performed at the employer's premises, is carried out away from those premises on a regular basis. The following basic characteristics of teleworking are derived from the agreement: it is voluntary (it cannot be unilaterally ordered), workers have the same rights as those working at the employer's premises, the employer must provide adequate equipment and personal data protection, respect the employee's privacy. provide him or her with all the necessary equipment and check that the worker meets the conditions for safety and health at work. In 2008, a Report on the implementation of the European social partners' Framework Agreement on Telework was published, which found

⁵ Framework Agreement on Telework, available at: https://resourcecentre.etuc.org/sites/default/files/2020-09/Telework%202002_Framework%20Agreement%20-%20EN.pdf

that the Framework Agreement on Telework had been successfully implemented in most EU Member States and EEA Countries⁶.

Although the rules on teleworking have been implemented in virtually all national legislation in recent years and the development of the Internet and other forms of digitalisation has had a significant impact on all employment relationships (give source of this affirmation), it can be seen that (until recently) teleworking was rarely done (give source of this affirmation). It is true that workers used machines, computers, robots and other smart devices at work, but the work was still done traditionally on the employer's premises and in relatively strictly defined work frames. The latter was also common for business meetings and other gatherings. Although technology has long enabled remote access to work computers and machines, cloud use, data transfer to private environments, real-time video conferencing meetings, electronic document signing, etc., these tools have been virtually unused in the context of employment law (give source of this affirmation).

In the first half of 2020, however, there was a significant change that had a significant impact on the further development of teleworking. The COVID-19 pandemic has caused, at minimum, temporary drastic transformations in work processes and introduced virtually 100% work from home in most sectors, at least for a limited period of time (give source of this affirmation). Due to several measures to prevent the spread of COVID-19, the work process ~~has~~ moved into different online environments. As in other sectors, people were forced to adapt to new working conditions practically overnight in higher education institutions and to carry out the entire pedagogical process, as well as all administrative and organizational work, remotely via the electronic network. Prior to the COVID-19 pandemic, employees at higher education institutions used e-mails and some learning environments in which they uploaded teaching materials. Those who were more technologically "advanced" may have published a short video of the lecture. In the post-Covid-19 era, the picture is completely different. Many lecturers publish various recordings and other video content, use remote access, collect electronic applications, seminar papers and keep various electronic records. For lectures and meetings (and in some

⁶ Commission of the European Communities, Commission Staff Working Paper, Report on the implementation of the European social partners' Framework Agreement on Telework, {COM (2008) 412 final}, Brussels, 2.7.2008.

cases even for knowledge testing) they use various tools that enable real-time face-to-face online communication, such as Zoom, MS Teams, Skype and others.

3 Individual Aspects of Cybersecurity

With the introduction of the Internet in labour law proceedings, questions were initially raised regarding the (in)permissibility of the use of the Internet and webmail for private purposes. Especially in the initial phase, many employees could not resist the temptation and played online games during working hours, read the news, visited adult websites, online stores, sent e-mails with entertainment content, etc. This kind of behaviour led to lower productivity that could jeopardize the work process of the employer. Namely, by inappropriate use of the Internet, employees could cause many problems to the employer in the initial phase of using the Internet, such as criminal and compensatory liability for downloading illegal content, harassment and other inappropriate behaviour, violation of copyright law, damage to the reputation of the employer. process due to the transmission of computer viruses and other malicious programs, etc. As a result, employers have had to establish certain rules regarding the level of tolerance regarding private internet browsing or the admissibility of private emailing and warn employees in various ways about the risks and dangers of using the Internet (Malte Niemann, 2002: 114-116). In addition to strict rules, some employers have also technically disabled access to private content on work computers.

With regards to the private use of the Internet and e-mail, the question of the admissibility of online supervision has been raised from the outset, as the employer can strongly interfere with the employee's right to privacy by controlling the use of the Internet and e-mail. The European Court of Human Rights in *Bărbulescu v. Romania* has decided that the employer has the right to control the private use of the Internet and e-mail, but not based on the adoption of a general policy permitting monitoring. This means that the employer must set out precise rules, outlining why, how and where employees may be monitored and explaining how any information gathered through monitoring may be used⁷.

⁷ *Bărbulescu v. Romania*, The European Court of Human Rights, Grand Chamber, (Application no. 61496/08, 5 September 2017.

If at first the threat to online security and negative consequences for the employer could be caused mainly by consciously inadmissible actions of employees (non-compliance with the rules regarding the use of the Internet for private purposes), telecommuting began to create completely new risks and challenges. Technological development and globalization have brought new challenges, especially in the field of personal data protection. The volume of collection and exchange of personal data has increased significantly, and individuals are rarely aware of the consequences of their actions. To protect individuals with regard to the processing of personal data, a General Data Protection Regulation has been adopted⁸, regulating detailed rules regarding data protection.

Online tools have significantly simplified the way people work, but they pose a serious security risk to the employer in the event of violation or misconduct. Namely, the employer can suffer great damage in the form of financial loss, negative consequences due to unwanted transmission of documents, business secrets and other data, and sanctions due to violations of personal data protection rules. Even the smallest error or deficiency in the system can pose a major security risk. Individual aspects of online security in connection with the employment relationship in higher education institutions can be divided into the following sections: 1) deletion or transmission of data due to error, 2) cyberattacks, 3) inadmissible control, and 4) unauthorized use of data.

We will briefly explain the above-mentioned sets of online security in the case of an employee of a higher education institution, and the above applies to professional as well as to pedagogical and scientific-research workers. Web clouds and e-learning environments allow employees to store a variety of data. In the case of professional staff, these are various financial, academic and administrative data, and in the case of pedagogical and research staff, especially personal data on students, teaching materials, student works, records of applicants for examinations, records of grades, etc. If the listed documents and data are located in the web cloud, there is a high risk of unwanted data deletion (especially if proper data backup is not provided) or unwanted transmission of data to ineligible persons. The risk is even greater in the case of joint documents (a document that can be edited by several people at the same

⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

time) and joint folders. The more people have access to the data, the greater the security risk.

The risk of online attacks (data intrusion and encryption) occurs especially in the case of remote access or in the case of downloading malicious software. Employees are the target of various (personalized) ways of stealing user data, phishing attacks, social engineering attacks, distributing malware, etc. Recently, attacks with data encryption for the purpose of extortion have become particularly common. Thus, we can read about many cases of employees confronted with a message on the screen: *“All your files are encrypted with RSA-2048 encryption. ... It’s not possible to recover your files without a private key. ... You must send us 0.7 Bitcoin for each affected PC or 3 Bitcoins to receive ALL Private Keys for ALL affected PCs.”* (Chuang, 2018). If an employee works on the premises of a higher education institution and uses a business computer, internet connection, licensed software with appropriate protection, etc. and at the same time respects generally known facts and employer policy (e.g., the fact that we do not open suspicious emails, do not transmit suspicious files, we do not open unknown and suspicious websites, etc.), cyberattacks should not occur in principle. However, working remotely is more problematic, as in this case, people use their own internet connections, in some cases also private computers, mobile phones and other devices that are not sufficiently secured.

In the case of higher education institutions, the issue of inadmissible supervision arises particularly in connection with the monitoring of the implementation of lectures, exercises, examinations and other obligations of study obligations. These are especially cases where a certain person (e.g. superior, student or a third party) is secretly involved in real-time communication. Perhaps less frequently, however, even in the case of higher education institutions, there is a risk of scrutiny in relation to meetings on business and other important decisions.

By publishing their own products (e.g. seminar work, examination papers, etc.) in online e-learning environments or sending them via e-mail, unauthorized use of data for various purposes may occur. Regarding the unauthorized use of copyrighted products, pedagogical and scientific or research workers are even more exposed, as their products (e.g. study materials, videos of lectures, research results, etc.) are even more sought after. In the case of distance learning, the risk of unauthorized use of

data is even greater, as participants in study programs can obtain data relatively easily (e.g. by inadmissible recording, storage of data from e-learning environments, etc.).

4 Mitigation of Risks

Regarding the stated risks in the field of labour law aspects of online security of higher education institutions, the question arises how to minimize individual risks and thus improve the online security of employees, students and other participants. We can consider that the existing rules and institutes of labour law adequately address this area, with the need to apply them appropriately. Workers must perform the work for which they have concluded an employment contract in accordance with the applicable legislation and with the required level of diligence. They must follow the instructions of the employer unless they lead to wrongdoing or omission. They must refrain from any action which, given the nature of the work they do, could harm the stated interests of the employer. They must protect business secrets and are liable for damages if the employer causes material or non-material damage resulting from their fault.

As a result, measures to mitigate security risks are primarily in the hands of the employer. By measures, however, we do not mean so many binding legal rules that would be included in an employment contract or in collective agreements at various levels, but rather in the preventive actions of the employer. A prerequisite for adequate online security in the workplace is the identification of security risks and the development of appropriate protocols. It is recommended that every employer (including in the field of higher education) adopt an appropriate security policy, which addresses the most common security risks related to the use of the Internet and electronic devices and provides ways (security protocols) to prevent or mitigate the consequences.

Even more important than the adoption of the security policy is the education of employees, e.g. knowledge of GDPR, constant warning of possible risks and mistakes, and the ongoing identification of new security risks. The fact is that employees do not (yet) have the appropriate knowledge to ensure online security, so it is even more important that they know the employer's security policy in detail, understand it and "take it for granted". It should be pointed out that cybersecurity professionals, who specialize in the field of online security, have an increasing role

in work environments, and it is expected that certain knowledge about online security due to the needs in work environments will be acquired in the educational process (De Zan & Di Franco, 2019).

5 Conclusion

We can conclude that the risks in the field of labour law aspects of online security are usually the result of careless or unwitting or deliberate behaviour of employees or the result of inappropriate business processes. We must be aware that in the age of digital technology, just one wrong or careless "click" can cause great damage and irreparable consequences. To reduce security risks, we must constantly identify hazards and educate employees on appropriate ways to use the Internet and electronic devices. In addition to knowing the security policy and security risks, it is extremely important that we are very careful and attentive when performing work, especially if we perform with a large amount of (personal) data, and if we perform work remotely. What future implications of labour law with the rise of artificial intelligence, notably (unsupervised) "deep learning"? For example, can one envisage a link between labour law and the need for an audit of algorithms and IA? e.g., <https://www.businessofgovernment.org/sites/default/files/Algorithmic%20Auditing.pdf>

References

- Chuang, Tamara, Pay us bitcoin or never see your files again: Inside the highly profitable underworld of ransomware, *The Denver Post*, 8 March 2018.
- Commission of the European Communities, Commission Staff Working Paper, Report on the implementation of the European social partners' Framework Agreement on Telework, {COM (2008) 412 final}, Brussels, 2.7.2008.
- De Zan, Tommaso, Di Franco, Fabio, *Cybersecurity Skills Development in the EU*, European Union Agency for Cybersecurity (ENISA), 2019.
- Malte Niemann, Jan, *Monitoring Internet and Email Usage - Germany: Surfing into Unemployment? Private Internet Use and Emailing under German Labour Law*, *Computer Law & Security Review*, Volume 18, Issue 2, 2002.
- Senčur Peček, Darja, Franca, Valentina, *From student work to false self-employment: how to combat precarious work in Slovenia?* in: Kenner, Jeff (ed.), Florczak, Izabela (ed.), Otto, Marta (ed.). *Precarious work: the challenge for labour law in Europe*. Cheltenham; Northampton: E. Elgar. 2019.

HUMAN RIGHTS AND CYBERSECURITY

ROK DACAR

University of Maribor, Faculty of Law, Maribor, Slovenia
rok.dacar@um.si

Abstract The connection between virtual learning environments and human rights can be seen in two ways. On the one hand, non-binding documents set some rights to be implemented by states regarding the functioning of the worldwide web (and consequently also virtual learning environments). On the other hand, intrusions into virtual learning environments may cause violations of human rights, mainly the right to personal data security and the right to privacy and family life. From the vast jurisdiction of the European Union Court of Justice and the European Court of Human Rights, one can find out the pre-conditions for such a district intervention to represent violations of human rights. The aim of this article is to disseminate the relevant know-how to all interested parties, especially students, teachers and other practitioners.

Keywords:

right to privacy
and family life,
virtual learning
environments,
right to personal
data security,
European Court of
Human Rights,
European Union
Court of Justice

1 Introduction

In the past decades, the Internet has grown from an effective work tool to a key component of our lives. Via the Internet, we purchase goods, watch TV programmes, meet partners, access cultural and educational content, and work. During the coronavirus pandemic, its importance grew additionally, as, for many of us, it became the only window to the world placed in isolation and lockdowns. Digital life became almost equal to actual physical life. It is, therefore, no surprise that the Internet can be an environment where serious violations of human rights can occur, while at the same time, the internet is essential for the enjoyment of several fundamental rights. The chapter clarifies some of the more current questions on the relationship between the Internet and human rights that are relevant to virtual learning environments. Firstly, the term cybersecurity and its meaning for society is briefly presented, followed by discussions about some rights connected to the use of the Internet established by the legally non-binding Convention on Human Rights and principles of the Internet. Furthermore, the chapter highlights potential violations of human rights connected to intrusions into virtual learning environments while concentrating on the right to privacy and family life and the right to personal data security, as determined by the Charter of Fundamental Rights of the European Union (henceforth: the Charter) and the European Human Rights Law. The chapter then presents the relevant case Law of the Court of Justice of the European Union (henceforth: CJEU) and the European Court of Human Rights (hereafter: ECHR). Finally, the chapter synthesises the most relevant points of the text.

2 Cybersecurity and Virtual Learning Environments

As the chapter is connected to the term cybersecurity, a short explanation of the subject is in order. There is no single definition of cybersecurity, but we can understand it as "security of systems, networks and programmes from computer attacks usually aiming at access, change or destruction of sensitive data, extortion of money or interruption of usual commercial flows¹". Thus, cybersecurity provides a safe virtual learning environment. Effective cybersecurity policies and measures are

¹ Cisco, What is Cybersecurity, accessible under: <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html> (6.6.2021).

important due to the generally high importance of the digital space in contemporary society, notably for the protection of various social and socio-technical subsystems. In the case of an intrusion into a virtual learning environment, the functioning of an educational system might be endangered (at a time when a vast part of learning activities is done through the Internet, it is not hard to imagine the destructive effect of a cyberattack disabling virtual learning environments), and theft of data (names of participants, e-mail addresses, theft of records of internet camera recordings, theft of uploaded documents, etc.).

2 Online Human Rights

»The Internet has become much more than just a communication tool, as it intertwines with the real world in numerous fields²«, human rights and basic liberties being especially relevant for this chapter. Due to this, the *Charter of Human Rights and Principles for the Internet* based on the Declaration of principles at the *WSIS*³ (*World Summit of the Information Society*) and at the Tunis Agenda of the *WSIS*⁴ were passed«. The Convention is not legally binding, and consequently, there are no obligations imposed on national states, the managers of websites, web browsers, etc. The adoption of the above-mentioned acts highlights the importance of the Internet. Also, it represents a domain of values helping us in the search for concrete legal solutions, where the rights mentioned have to be seen as orientations. Of course, in practice, these rights cannot always be guaranteed in all cases. The Convention lists ten basic rights and principles connected to using the Internet (online human rights) that may be transferred to virtual learning environments. They are⁵:

1. Universality and equality – equality and personal freedom of all have to be protected and met on the Internet (*all participants of the virtual learning environment have, e. g., an equal right to participate in debates, discussions, ...*)

² Moise, *ibidem*, p. 161.

³ Two-part world summit of the information society took place within the UNO in 2003 in Geneva and in 2005 in Tunis. At the summit in Tunis the Tunis Declaration proposed by the Internet Governance Forum was adopted and a special platform for the worldwide web, in which various stakeholders were involved, was established.

⁴ Moise, *ibidem*, p. 162.

⁵ Taken from: Internet Governance Forum, *The Charter of Human Rights and Principles for the Internet*, accessible under:

<https://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf> (6.6.2021).

2. Availability/Accessibility – everybody has an equal right to access a safe and open internet (*all students have a right to access a virtual learning environment disregarding their personal background*)
3. Neutrality – everybody must have access to content on the Internet without prioritisation, discrimination, censoring, filtering and control of traffic (*e.g., certain topics of a virtual learning environment must not be prohibited from discussion*)
4. Respect of human rights – as the Internet is a space for fostering, protecting human rights, everybody must respect the human rights of everyone else in the use of the Internet (*users of a virtual learning environment, for example, are not allowed to humiliate their peers*)
5. Right of expression – everybody has a right to express opinions on the Internet and obtain and seek information without arbitrary interference and surveillance. Everybody has a right to anonymous communication on the Internet (*users of a virtual learning environment may freely express their views on a given topic*)
6. Life, freedom and security – on the Internet, the right to life, freedom and safety have to be respected; these rights may not be violated to interfere with the human rights of other people (*in virtual learning environments there must not be any incitement of dangerous activities*)
7. Privacy – everybody has a right to privacy in the use of the Internet. This includes the right to use the Internet without being subject to surveillance. The individual to whom the data refers must have control over the collecting, storing and use of his or her personal data (*activities in a virtual learning environment are not allowed to be controlled by a third party/organisation*)
8. Diversity – on the Internet, cultural and language diversity must be fostered, and technical innovations should facilitate this (*fostering these values in a virtual learning environment*)
9. Standards of good management – an architecture of the Internet shall be built on standards allowing the simplification and inter-operability of the working environment (*user of the virtual learning environment X can freely access the virtual learning environment Y and transfer its content*)
10. Good management – human rights and social justice shall be the core values on which the Internet functions.

3 Potential Violations of Human Rights Through Virtual Learning Environments

As all of us spend more and more time on the Internet (this almost radically increased during the pandemic of Covid-19 with virtual lectures, video meetings, home office, and such like), resulting in numerous possible violations of human rights by a state. These violations can be caused mainly by state surveillance of the use of the Internet, in our case of virtual learning environments. In connection to this, all of us remember the *Patriot Act*⁶ in the USA, which widened the possibilities of surveillance of the cyberlives of citizens after September 11. However, one does not need to go over to the Atlantic Ocean to find an act widening limits of legal surveillance over the Internet, neither do we have to go far back in history, as we may look at France, where, following the terrorist attacks on the satiric revue *Charlie Hebdo* the *Loi relative au renseignement*⁷ (an approximate translation might be the Law on Intelligence Activities) was adopted, allowing for a broad and non-discriminatory collection of metadata on the Internet based on searches by individual users, without providing sufficient judicial protection. The stated purpose of both laws is the defence of society from terrorism, that was a clear and present danger at the time of their adoption (i.e., providing for public safety) and not the seeking of non-democratic or autocratic goals. In connection with the two above Acts, questions on the respect of human rights and fundamental freedoms on the Internet (cyberspace) have been raised. Surveillance of user activities in virtual learning environments reaches into numerous human rights areas, like the right to privacy and family life and the right to personal data security are the most endangered rights⁸.

⁶ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, accessible: <https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act> (6.6.2021)

⁷ Loi n° 2015-912 du 24 juillet 2015 relative au renseignement (1), accessible: <https://www.legifrance.gouv.fr/loida/id/JORFTEXT000030931899/> (6.6.2021)

⁸ Also interferences in the right to expression, gathering, interferences into various political rights are imaginable, etc.

3.1 Right to Privacy and Family Life and the Right to Protection of Personal Data

The right to privacy and family life is provided by article 8 of the European Convention on Human Rights (henceforth: EHRC) and article 7 of the European Charter on Human Rights (hereafter: the Charter). Article 8 of the EHRC and article 7 of the Charter have the same text, with only the word »correspondence« used by EHRC being replaced by »communication« in the Charter. The reason for the change of words is probably the technological progress within the five decades that passed, from the writing of the text of the ECHR to the adoption of the Charter. In the Charter, the text of article 7 is »Everyone has the right of respect for his or her private and family life, home and communications.«, and in the EHRC », Everyone has the right of respect for his personal and family life, his home and his correspondence.«, whilst article 8 EHRC contains an additional second section determining that »there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others«. The word »correspondence« is interpreted widely by the ECHR. Among others, it entails e-mails⁹, the use of the Internet¹⁰, data stored on computer servers¹¹, etc. The text of the article refers to four values: privacy, family life, inviolability of housing and inviolability of communications or correspondence, respectively. In connection to the security of virtual learning environments, the most relevant of them is the right to inviolability of communications, despite the possibility that an intrusion might also violate another value among the four previously cited. Despite the right to the protection of personal data not being directly mentioned in the ECHR, the ECHR has been guaranteeing it through article 7. In the Charter, the right to protection of personal data is guaranteed by article 8, which states that everyone has the right to the protection of personal data concerning him or her (section 1), that data must be processed fairly for specified purposes, and on the basis of the consent of the person concerned or some other legitimate basis laid

⁹ ECHR, *Copland vs. UK* (62617/00) from 3.7.2007, para. 41 in ECHR, *Barbulescu vs. Romania* (61496/08) from 5.9.2017, para. 72.

¹⁰ ECHR, *Copland vs. UK* (62617/00) from 3.7.2007, para. 41-42.

¹¹ ECHR, *Wieser and Bicos Beteiligungen GmbH vs. Austria* (74336/01) from 16.10.2007, para. 45.

down by law and everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified (section 2). Finally, compliance with these rules shall be subject to control by an independent authority (section 3). On the EU level, the right to personal data protection is operationalised mainly through the provisions of the GDPR (*General Data Protection Regulation*) that operationalises various aspects of personal processing data and is presented in more detail in another chapter of this manual.¹²

3.2 Jurisdiction of the ECHR and EUCJ

Since December 2009, when the Charter gained binding value, the CJEU has been competent to decide on violations of human rights guaranteed by the Charter and committed by institutions and bodies of the EU and member states when applying EU law¹³. Where the Charter contains rights that are analogue to the rights from the EHRC, their contents and range are the same as the one determined by the EHRC, and a higher level of security can be assured¹⁴. If a member of the Council of Europe violates the right to privacy and family life of a citizen, this individual can file a complaint to the ECHR after seizing national courts of justice. The same violation can also be addressed by the CJEU, but only if the violation was committed by an EU member state (all EU member states are also members of the European Council) in the execution of European law. If a violation is committed by a body or institution of the EU, the individual could only seize the CJEU, as the ECHR is not competent for conflicts against European institutions and bodies. As stated, the ECHR is dealing with violations of the right to protection of personal data based on article 8 of the ECHR. The ECHR always interpreted the right to privacy and family life very widely. Thus, in the case of *López Ostra vs. Spain*,¹⁵ it was decided that the right to privacy and family life of the plaintiff was violated by the setting up of a cleaning facility just a short distance from her house, which decreased the quality of her residence and consequently her life.

¹² See Aljoša Polajžar, Personal Data Security (Directives of Education Institutions and Students).

¹³ Article 51 section 1 Charter.

¹⁴ Article 52 section 3 Charter.

¹⁵ ECHR, *López Ostra vs. Spain* (16789/90) from 9.12.1994.

Regarding the Internet, the ECHR found that, due to its general availability and the capability to store a vast amount of information, it plays an important role in enabling the public to obtain information and news of a public character¹⁶, but at the same time poses a danger for human rights (mainly for the right to privacy and family life) that is higher than the one from traditional media¹⁷. In connection to cybersecurity, the case of *Breyer vs. Germany*¹⁸ must be mentioned, where ECHR recognised that in the context of the fight against organised crime and terrorism and in light of contemporary telecommunication methods and the changes in the communication behaviour of individuals, investigative methods should also be changed. In the case of *Szabó and Vissy vs. Hungary*¹⁹ the ECHR similarly found that regarding the forms of modern terrorism, it is totally understandable that states use the most advanced technologies of mass surveillance of communication with the aim of preventing terrorist attacks. Still, the legal regulation of such measures must contain safeguards against discrimination, and unlimited surveillance must not take place. This was once again stressed by the ECHR in the case of *Zaharov vs. Russia*²⁰. In connection to the protection of family life and privacy, the case of *Rotaru vs. Romania*²¹ is also important. The ECHR found that the lack of clarity of legal regulation regarding terms of storage and use of data about the privacy of citizens by public authorities represents a violation of the rights guaranteed by the Convention. In the case of *S. and Marper vs. the United Kingdom*²² the ECHR stressed that modern scientific methods for crime prevention must not be used at any price, and careful balancing of the positive effects of their use and the consequences to the right to privacy is needed. Every state has a leading role in developing such technologies and has a special responsibility to ensure an appropriate balance between the general need of society for crime prevention and the rights of individuals. The term »modern scientific technologies« must be interpreted as including technologies that have the potential to violate the right to family life and privacy and to the protection of personal data, by intrusions in virtual learning environments. In the case of *Gaughran vs. the United Kingdom*, the ECHR stressed that national courts, when deciding on the necessity of a measure violating the right to

¹⁶ ECHR, *Times Newspapers Ltd vs. United Kingdom* from 10.6.2009, para. 27.

¹⁷ ECHR, *M.L. and W.W. vs. Germany* (60798/10 and 65599/10) from 28.9.2018, para. 91.

¹⁸ ECHR, *Breyer vs. Germany* (50001/12) from 30.1.2020, para. 88.

¹⁹ ECHR, *Szabó and Vissy vs. Hungary* (37138/14) from 12.1.2016, para. 68, 73-75.

²⁰ ECHR, *Zaharov vs. Russia* (47143/06) from 4.12.2015, para. 302-305.

²¹ ECHR, *Rotaru vs. Romania* (28341/95) from 4.5.2000, para. 50.

²² ECHR, *S. and Marper vs. United Kingdom* (30562/04 and 30566/04) from 4.12.2008, para. 112.

privacy and family life and the right to personal data protection of an individual, must consider the complexity of the newest technological achievements and their influence²³. Furthermore, in the case of *Klass vs. Germany* the ECHR decided that data collection on citizens by the government limited to judicial controls (e.g., undercover investigation approved by the decision of an investigating judge) does not represent a violation of the rights guaranteed by the Convention. The case *Digital Rights Ireland Ltd. vs. Minister of Communications*²⁴ must also be mentioned, where the CJEU established that the metadata collection on individuals violated their right to the protection of personal data, as it was possible to obtain personal data from metadata. In the case of *Schrems* 2²⁵, the CJEU examined the forwarding of personal data from an EU member state to the USA and decided that the Decision on the Personal Shield was illegal, as it had doubts that the level of personal data protection in the USA was comparable with the one guaranteed in the EU. In addition, the case of *Tele2/Watson*²⁶ must be mentioned, where the CJEU decided that »national legislation introducing storage of all traffic and localisation data of all registers of electronic communication users for the purpose of fighting crime generally and non-discriminatory, violates the right to privacy and the right to the protection of personal data. Access to such data has to be limited only to cases of fighting against severe crime. Still, even in that case, an *ex ante* supervision by an independent judicial or administrative institution has to be provided for²⁷«.

3.3 What Intervention is Allowed?²⁸

Violations of fundamental rights via the intrusion into virtual learning environments are extremely rare. Despite this, based on the above-mentioned case Law, one may conclude what conditions such an intervention must meet to be allowed. In order not to represent a violation of a fundamental right, such an intervention must be, be (i) non-arbitrary, (ii) transparent and (iii) must contain sufficient safeguards.

²³ ECHR, *Gaughram vs. United Kingdom* (45245/15) from 13.6.2020, para. 96-98.

²⁴ EUCJ, *Compiled matters C-293/12 and C-594/12*.

²⁵ EUCJ, *C-311/18*.

²⁶ EUCJ, *C-698/15*

²⁷ Privacy International, *Tele2/Watson*, accessible: [https://privacyinternational.org/taxonomy/term/410\(6.6.2021\)](https://privacyinternational.org/taxonomy/term/410(6.6.2021)).

²⁸ Pre-conditions partially taken from: Cross, *ibidem*, p. 629-633.

- (i) The fundamental rights of individuals could be violated via an intrusion into a virtual learning environment only where some justifiable reason would exist (e.g., a potential terrorist activity, a decision by an investigating judge, and likewise). However, a general gathering of personal data of all users of the virtual learning environment can never be allowed. For example, the intrusion into a virtual learning environment could be justified if its users were potentially preparing terrorist activities (e.g., surveillance concerning jihadist websites via an Internet browser or those who seek computer codes connected to terrorism).
- (ii) There must be at least some degree of transparency in the execution of measures with the aim of preventing violations. This can be reached by surveillance of the way of carrying out-measures from an independent institution (e.g., a parliamentary committee). This mainly means that information on the execution of the measures, and technical processes and likewise would not be known only to a narrow circle of people, but also to some external supervisory body.
- (iii) This pre-condition, to a certain degree, is connected to the condition of transparency, despite its broader range. While transparency only means that some institution supervises the legality of the measure *ex-post*, the presence of legal safeguards could be satisfied, for e.g., by including the judicial branch in the execution or control of the measures. In connection to this, the French case *Loi relative au renseignement* is to be mentioned as lacking measures on sufficient supervision, as in France, the prime minister directly decides on the more invasive measures and the independent authority (where legal jurisdiction is poorly represented) merely gives advice to him.

If some measure and the execution of it satisfies the previously mentioned pre-conditions, it means that it probably does not violate the right to privacy and family life, but it does not yet mean that it does not violate the right to personal data protection. For a measure not to violate the right to the protection of personal data further conditions have to be met, namely the measure must (iv) be determined specifically enough ahead, and (v) surveillance of its execution by an independent institution must also be present.

- (iv) An exact determination of data to be collected is necessary to stop possible violations that might occur if all sorts of data could be obtained. A violation might happen, if, for example, the data on the content of the communication between a lawyer and a client, a reporter and his or her confidential source, etc. would be collected. As such communication (in principle) is not done within virtual learning environments, this condition is of limited relevance to this article.
- (v) Article 8 section 3 of the Charter explicitly requires that the respect of the right to the protection of personal data is supervised by an independent authority. Demand for supervision by an independent authority is mainly contained in the pre-conditions under (ii) and (iii), already mentioned above.

These conditions are not permanently set in stone, and in line with the margin of appreciation doctrine, a certain freedom in the carrying out of the measures is granted to the member state of the Council of Europe, whilst the states must achieve »a fair relation between protection of the general public interest and respect of human rights, where the latter has to be subject to special attention²⁹«.

4 Conclusion

This article explained that the development of the Internet has a potential influence on fundamental rights. On the one hand, programme documents emerge determining (online human) rights to guarantee undisturbed, equal, fair, etc. access to the Internet and consequently also to virtual learning environments. On the other hand, the Internet offers yet unseen possibilities for the violations of human rights. The contribution mainly dealt with the right to privacy and family life and the right to the protection of personal data. Still, one could also imagine intrusions into virtual learning environments violating other human rights, e.g., the freedom of association and the freedom of expression. In the past decade, the CJEU and the ECHR developed a vast body of case Law. Based on it we can conclude under which conditions intrusions into virtual learning environments would be allowed and even more importantly, what conditions must be met by an intervention, so it does not

²⁹ ECHR, subject »Relating to certain aspects of the Laws on the use of languages in education in Belgium« vs. Belgium (474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64), from 23.7.1968, chapter B, para. 5.

represent a violation of human rights. It must be stressed again that intrusions into the cybersecurity of virtual learning environments are extremely rare.

References

- »Relating to certain aspects of the Laws on the use of languages in education in Belgium« vs. Belgium (474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64) from 23.7.1968.
- Adrian Cristian Moise: Cybersecurity and Human Rights, v: Revista Universul Juridic 2016, no. Supplement (2016).
- Cisco, What is Cybersecurity, accessible under: <https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html> (6.6.2021).
- ECHR, Barbulescu vs. Romania (61496/08) from 5.9.2017.
- ECHR, Breyer vs. Germany (50001/12) from 30.1.2020, para 88.
- ECHR, Copland vs. UK (62617/00) from 3.7.2007.
- ECHR, Gaughram vs. United Kingdom (45245/15) from 13.6. 2020, para. 96-98.
- ECHR, López Ostra vs. Spain (16789/90) from 9.12.1994.
- ECHR, M.L. and W.W. vs. Germany (60798/10 and 65599/10) from 28.9.2018, para. 91.
- ECHR, Rotaru vs. Romania (28341/95) from 4.5.2000, para. 50.
- ECHR, S. and Marper vs. United Kingdom (30562/04 and 30566/04) from 4.12.2008, para. 112.
- ECHR, Szabó and Vissy vs. Hungary (37138/14) from 12.1.2016, para. 68, 73-75.
- ECHR, Times Newspapers Ltd vs. United Kingdom from 10.6.2009, para. 27.
- ECHR, Wieser and Bicos Beteiligungen GmbH vs. Austria (74336/01) from 16.10.2007.
- ECHR, Zaharov vs. Russia (47143/06) from 4.12.2015, para 302-305.
- Internet Governance Forum, The Charter of Human Rights and Principles for the Internet, accessible under: <https://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf> (6.6.2021).
- Jennifer Cross: Cybersecurity and the Rights of the Internet User in France, v: Georgia Journal of International and Comparative Law, let. 45, no. 3 (2017).
- Loi n° 2015-912 du 24 juillet 2015 relative au renseignement (1), accessible: <https://www.legifrance.gouv.fr/lo da/id/JORFTEXT000030931899/>.
- Privacy International, Tele2/Watson, accessible: <https://privacyinternational.org/taxonomy/term/410> (6.6.2021).
- EUCJ, C-311/18.
- EUCJ, C-698/15
- EUCJ, Compiled matters C-293/12 and C-594/12.
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, accessible: <https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act>.

COPYRIGHT PROTECTION IN EDUCATION

KRISTJAN ZAHRASTNIK

University of Maribor, Faculty of Law, Maribor, Slovenia
kristjan.zahrastnik@um.si

Abstract Respect of copyright encompasses all levels of education. Starting with a simple homework in elementary school, all way through to a diploma thesis of a study programme. This topic also refers to teachers and professors in research and the pedagogical process. Therefore, the author wants this chapter to stress essential aspects of copyright. In the beginning, the legal framework of copyright in the EU is presented. Then, a description of the term plagiarism, citing of copyrighted work providing for respect of another author's work, forms of copyright in education and research, the question of ownership of copyright in labour relations, and exceptions from use of copyright in teaching or research follows.

Keywords:
copyright in
education,
plagiarism,
citing, forms of
copyright in
education,
copyright in the
EU

1 Introduction

As copyright in the EU is regulated by many directives allowing Member States a specific liberty in implementing the rules, copyright differs between EU Member States despite the same core. Thus, as an introduction, the legal framework of copyright law in the EU is presented. Then, a description of the most relevant aspects of copyright in education follows. The topic addressed in the framework of copyright in education encompasses the term plagiarism, citing of copyright providing for respect of another author's work, forms of copyright emerging in education and research, the question of ownership of copyright in labour relations and exceptions in the use of copyright in teaching or research. Many questions are regulated on a national level in terms of copyright in education. Therefore in the course of the text, Slovenian law will be used to represent an exemplification pattern of EU regulation.

2 Copyright Law in the EU

Copyright means the right of authors to literature, scientific works, and works of art.¹ It must be stressed that copyright in the world is not submitted totally to a unique regulation. Still, EU Member States have a set of common ground regarding certain aspects of copyright in numerous legal acts. Legal acts addressing copyright in the Member States are listed in the table below.

European Union Intellectual Property Office Observatory (EUIPO) offers answers to the 15 most frequently asked questions in national and in English for the 27 Member States. These questions regarding respect to the copyright in education include:

- “Under what conditions may I use a work under copyright created by someone else? I was told that the use of works created by others is just a citation and, as such, is always allowed.

¹ Compare with article 1 of Copyright and related Rights Act (*Zakon o avtorski in sorodnih pravicah*) (hereinafter ZASP), Official Gazette RS, no. 16/07.

- Is it allowed to upload a work under copyright from the Internet, and in doing this, is it relevant what technology I use and if I upload only parts of such a work?
- How do I know whether a work under copyright is offered online in a legal or illegal way?"²

Table 1: List of EU copyright legislation.

Source: European Commission, Shaping Europe's digital future, The EU copyright legislation, accessible under: <https://digital-strategy.ec.europa.eu/en/policies/copyright-legislation> (25. 6. 2021).

Name	Date	Area of application
Directive 2001/29/EC	22 May 2001	Directive on the harmonisation of certain aspects of copyright and related rights in the information society
Directive 2006/115/EC	12 December 2006	Directive on rental rights and lending rights and on certain rights related to copyright in the field of intellectual property
Directive 2001/84/EC	27 September 2001	Directive on the resale right for the benefit of the author of an original work of art
Council Directive 93/83/EEC	27 September 1993	Directive on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission
Directive 2009/24/EC	23 April 2009	Directive on the legal protection of computer programmes
Directive 2004/48/EC	29 April 2004	Directive on the enforcement of intellectual property rights
Directive 96/9/EC	11 March 1996	Directive on the legal protection of databases
Directive 2011/77/EU	27 September 2011	Directive amending Directive 2006/116/EC on the term of protection of copyright and certain related rights
Directive 2012/28/EU	25 October 2012	Directive on certain permitted uses of orphan works (Text with EEA relevance)
Directive 2014/26/EU	26 February 2014	Directive on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market
Directive (EU) 2017/1564	13 September 2017	Directive on certain permitted uses of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired, or otherwise print disabled and amending Directive 2001/29/EC on the harmonisation of certain

² European Union Intellectual Property Office Observatory – EUIPO, FAQs on Copyright, Pogosto zastavljena vprašanja o avtorskih pravicah, accessible under: <https://euipo.europa.eu/ohimportal/sl/web/observatory/faqs-on-copyright-sl> (27. 6. 2021).

Name	Date	Area of application
		aspects of copyright and related rights in the information society
Regulation (EU) 2017/1563	13 September 2017	Regulation on the cross-border exchange between the Union and third countries of accessible format copies of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are blind, visually impaired, or otherwise print-disabled
Regulation (EU) 2017/1128	14 June 2017	Regulation on cross-border portability of online content services in the internal market
Directive (EU) 2019/790	17 April 2019	Directive on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC
Directive (EU) 2019/789	17 April 2019	Directive of laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes, and amending Council Directive 93/83/EEC ^{3,4}

3 Plagiarism

3.1 Forms of Plagiarism

Participants in education must respect copyright in education (e.g., elementary school children, pupils, and students) as well as their educators (e.g., teachers and lecturers). Disrespect of copyright results in its violation. One of the forms of violation that are frequent, mainly in education, is plagiarism or presentation of another author's work as one's own. Plagiarism shows up mainly in the following forms of copyright violations:

- Copying another author's texts without naming the author or source,
- Copying another author's thoughts without naming the person,⁵

³ Three additional instruments (DIRECTIVE 87/54/EEC of 16 December 1986 on the legal protection of topographies of semiconductor products; Council Decision 94/824/EC of 22 December 1994 on the extension of the legal protection of topographies of semiconductor products to persons from a Member of the World Trade Organization and Council Decision 96/644/EC of 11 November 1996 on the extension of the legal protection of topographies of semiconductor products to persons from the Isle of Man) harmonise legal protection of topography of agricultural products.

⁴ Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) and Directive 98/84/EC of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, also contain provisions of relevance for enforcement of copyright.

⁵ Janez, Biblioblog, Plagiatorstvo in njegovo odkrivanje, accessible under:

- Copying a picture, sound, music sheet, computer software, sketches, or plans of another author without naming the person or without naming the source,⁶
- Copying another author's text or thought to such an extent that it forms a larger part of the new work (without citing the name of the author or source),
- Copying thoughts or texts and changing words in a text without naming the author or source,
- False naming (e.g. leaving out quotation marks, giving false data) of a source or an author⁷
- Translation of a work under copyright from another language without naming the author or source.⁸

The most common forms of plagiarism are the acceptance of parts of a text, images, graphs, tables, etc., from works of another author without their indication and taking over parts of another author's work, where minor changes and adaptations are made (replacement or modification of word order, sentence rearrangement, merging of another author's and one's own text) without a clear indication of the original author's work.⁹

Ghostwriting refers to actions where a person creates text for others without claiming copyright of the work (e.g., a so-called ghost writer prepares a final paper in exchange for money on the student's instructions, which the student claims as his or her own). This is not plagiarism, but it is nevertheless an act that is not allowed in education.¹⁰

The term self-plagiarism refers to the re-identical use of one's own text, which has already been previously published, without the author referring to previous work.¹¹

<https://www.biblioblog.si/2011/03/plagiorstvo-in-njegovo-odkrivanje.html> (13. 6. 2021).

⁶ Ivan Kanič, Knjižničarske novice, Plagiorstvo in njegovo preprečevanje, accessible under <http://old.nuk.uni-lj.si/knjiznicarskenovice/v2/podrobnostClanek.aspx?id=1202> (13. 6. 2021).

⁷ Janez, Biblioblog, Plagiorstvo in njegovo odkrivanje, accessible under:

<https://www.biblioblog.si/2011/03/plagiorstvo-in-njegovo-odkrivanje.html> (13. 6. 2021).

⁸ Milan Ojsteršek, SlideServe, Preverjanje podobnosti vsebin v e-izobraževanju, accessible under:

<https://www.slideserve.com/teagan-moss/preverjanje-podobnosti-vsebin-v-e-izobra-evanju> (13. 6. 2021).

⁹ Ivan Kanič, Knjižničarske novice, Plagiorstvo in njegovo preprečevanje, accessible under <http://old.nuk.uni-lj.si/knjiznicarskenovice/v2/podrobnostClanek.aspx?id=1202> (13. 6. 2021).

¹⁰ Debora Weber-Wulf (2014). False feathers: A Perspective on Academic Plagiarism. Springer. p. 14.

¹¹ Ivan Kanič, Knjižničarske novice, Plagiorstvo in njegovo preprečevanje, accessible under <http://old.nuk.uni-lj.si/knjiznicarskenovice/v2/podrobnostClanek.aspx?id=1202> (13. 6. 2021).

If the author has not transferred the material copyright of the text when it is published in a book or article, he or she has the right to use it again. Copyright, in this case, does not provide for sanctions, nor is it plagiarism, but such re-use of the text should be marked as a violation of the ethics of scientific research.¹²

Plagiarism can be committed intentionally and through negligence (superficiality or ignorance).¹³ Intention or unintentional plagiarism does not affect its presence but can be considered in legal proceedings when imposing a sanction.¹⁴ The extent of plagiarism is also not relevant to its presence; namely, even one sentence (key sentence or thought) can be qualified as appropriating another author's work as one's own (plagiarism).¹⁵

3.2 Consequences of Plagiarism

The consequences of plagiarism are:

1. Academic sanctions in the framework of legal proceedings of higher education institutions may mean the revocation of the acquired professional or scientific title.
2. Ethical sanctions that result in inappropriateness to perform their work or functions (politicians, senior officials, higher education teachers, etc.).¹⁶
3. A lawsuit for damages by an author whose copyright has been unjustifiably infringed.¹⁷

¹² Debora Weber-Wulff (2014). *False feathers: A Perspective on Academic Plagiarism*. Springer. p. 13.

¹³ Ivan Kanič, *Knjižničarske novice, Plagiatorstvo in njegovo preprečevanje*, accessible under <http://old.nuk.uni-lj.si/knjiznicarskenovice/v2/podrobnostClanek.aspx?id=1202> (13. 6. 2021).

¹⁴ Tomaž Keresteš (2017). *Akademski plagiat v Avtorska dela na univerzi* (ed. Martina Repas). Univerzitetna založba Univerze v Mariboru. p. 116.

¹⁵ Polona Tominc, Vladimir Drozg, Milan Ojsteršek, Nataša Samec, Bernarda Korez, Doroteja Kardum and Rok Hržič (2012). *Preverjanje plagiatorstva na UM*. Accessible under https://www.um.si/studij/splosno/Documents/Preverjanje%20plagiatorstva%20na%20UM%20-%20delovno%20gradivo_18_9_2012.pdf (13. 6. 2021), p. 1.

¹⁶ Tomaž Keresteš (2017). *Akademski plagiat v Avtorska dela na univerzi* (ed. Martina Repas). Univerzitetna založba Univerze v Mariboru. p. 103, 104.

¹⁷ Ivan Kanič, *Knjižničarske novice, Plagiatorstvo in njegovo preprečevanje*, accessible under <http://old.nuk.uni-lj.si/knjiznicarskenovice/v2/podrobnostClanek.aspx?id=1202> (13. 6. 2021).

3.3 How to Respect Copyright in Education

It is allowed to paraphrase and summarise another author's works, but under the condition of appropriate citation of the text or source, as it is a presentation of another author's thoughts, data, etc. The primary guideline for avoiding plagiarism is when the writer is not the original author of the text or its constituent part (e.g., sentence, pictorial material, graph, table, etc.), the author's work used must imperatively be cited.¹⁸

The Court of Justice has already ruled in certain cases on the use of copyright in education. Directives 2001/29/EC regulate acts of reproduction and communication of a work of authorship in Articles 2 and 3. Reproduction and communication of the copyrighted work to the public by a third party requires the prior consent of the original author. When, for example, a hyperlink of a website is published in a copyrighted work, which refers to the copyrighted work on another website, published with the prior consent of the copyright holder, it is not a matter of public communication, as the copyright holder may be published on the website in question, the work is simply withdrawn, making the cited hyperlink inoperable. For this reason, in this case, we cannot talk about communicating the author's work to the public. On the contrary, this means that the online publication of the author's work on another website is considered a new communication to the public, which is independent of the original communication, even if it is, for example, a photograph previously published without restrictions on its transfer and with the permission of the copyright holder. Accordingly, it is not allowed, for example, to use a photograph in a seminar paper without the authorisation of the copyright holder if the seminar paper is to be published on another publicly accessible website (e.g., the school website), even if the photograph cites its author.¹⁹

Due to the possible sanction of revoking an acquired title, attention should be paid to the respect of copyright when preparing the final work in higher education. Thus, the student must (1) respect copyright, (2) comply with the rules of the higher education institution on quoting or citing sources and literature; and (3) follow the supervisor's instructions. On the other hand, the supervisor of the final work must

¹⁸ Ibidem.

¹⁹ Case C-161/17, Land Nordrhein-Westfalen vs. Dirk Renckhoff, from 7 August 2018, ECLI:EU:C:2018:634, Points 7, 29, 44, 47.

(1) pay attention to the fact that the student is familiar with the guidelines and rules regarding citation or citation of sources and literature and that it respects the copyright, (2) professionally and carefully review the final work, and (3) check the text for possible plagiarism. Every higher education institution, whether at the level of universities or faculties, must have clear guidelines for preventing plagiarism.²⁰ Clearer and more detailed rules than the rules of citation or citations of sources and literature, respectively, make it easier for authors of final works to respect copyright and easier for supervisors to monitor their possible violations.

4 Citation or Naming of the Author's Work

The best way to reduce, if not eliminate, plagiarism and encourage the respect of copyright is to follow the guidelines and rules that apply to citations or naming of sources and the literature. Every higher education institution has rules at the university or faculty level, which students must follow when preparing their final theses or assignments.

As there are many ways to cite, guidelines and policies differ, we can nevertheless identify a common denominator that typically occurs in the same type of work cited, regardless of the method of citation:

- Books: author, book title, edition number or notebook, publisher, and year of publication.
- Chapter published in a multi-author book: author of the chapter, title of the chapter, editor of the book, title of the book with data (see the previous indent), and volume of the chapter by pages.
- Articles in journals: author, title of the article, name of the journal, year of publication, year and issue number in the year, and volume of the article.
- Websites: author, website name, subtitle or the title of the website article, the date of publication, the page number (where possible), and the date of access to the page.²¹

²⁰ Polona Tominc, Vladimir Drozg, Milan Ojsteršek, Nataša Samec, Bernarda Korez, Doroteja Kardum and Rok Hržič (2012). Preverjanje plagijatorstva na UM. Accessible under https://www.um.si/studij/splosno/Documents/Preverjanje%20plagijatorstva%20na%20UM%20-%20delovno%20gradivo_18_9_2012.pdf (17. 6. 2021), str. 2.

²¹ Univerzitetna knjižnica Maribor, Citiranje, accessible under: https://ukm.um.si/citiranje#_ftnref1 (18. 6. 2021).

This information is given either in the notes or in the list of references and sources, depending on the method of citation. In (current or final) notes or the footnote in parentheses, respectively, depending on the method of citation must always indicate the page number where the cited content is located, provided that the author's work is divided into pages. The text quoted literally must always be given in quotation marks. Appropriate citation ensures its purpose, which is primarily reflected in ensuring respect for copyright. It also allows for the verifiability of summarised, paraphrased, or literally copied content.

It is also worth noting the rule that generally known facts (e.g., the capital of a country) do not need to be cited. In this case, the author does not need to refer to the Constitution, which determines the capital of the state (e.g., Article 10 of the Constitution of the Republic of Slovenia²² stipulates that Ljubljana is the capital of Slovenia).

The most common ways of quoting are considered to be:

- APA, accessible under the following link: <https://apastyle.apa.org/>;
- AMA, accessible under the following link: <https://www.amamanualofstyle.com/>;
- Chicago, accessible under the following link: <https://www.chicagomanualofstyle.org/home.html>;
- IEEE, accessible under the following link: <https://ieeauthorcenter.ieee.org/wp-content/uploads/IEEE-Reference-Guide.pdf>; and
- MLA, accessible under the following link: <https://style.mla.org/>.²³

5 Forms of Copyrighted Works in Education

Qualifying elements of the author's work are:

- creation,
- the field of literature, science, and art,

²² *Ustava Republike Slovenije*, Official Gazette RS, no. 33/91-I.

²³ Univerzitetna knjižnica Maribor, Citiranje, accessible under: https://ukm.um.si/citiranje#_ftnref1 (18. 6. 2021).

- spirituality,
- expressiveness,
- individuality.²⁴

Copyright in a copyrighted work is created at the moment of the creation of the work.²⁵ Examples of copyrighted works are determined by the second paragraph of Article 5 of the ZASP, which along with several copyrighted works, also highlights (1) spoken works, such as, e.g., speeches and lectures; (2) written works, such as, e.g., articles, manuals, studies, and computer programs; (3) works of art, such as pictures and graphics, and (4) presentations of a scientific, educational or technical nature (technical drawings, plans, sketches, tables, expert opinions, plastic presentations and other works of the same nature). ZASP specifically stipulates that ideas, principles, discoveries, and official texts from the legislative, administrative, and judicial fields, as well as folk literary and artistic creations, are not protected by copyright.²⁶

Lectures within the pedagogical process at educational institutions are considered an author's work (ZASP explicitly cites them as an example of an author's work). Regarding PowerPoint slides, transparencies, and other material used as an aid in conducting lectures, there is no single answer as to whether it is a copyrighted work or not. The definition of an author's work varies from case to case. The lecture notes are, in fact, valid for their reproduction, which is why they are marked as the lecturer's work. The reproduction itself does not constitute a violation of copyright, especially if it is a reproduction that is in accordance with copyright (e.g., private reproduction within the framework of article 50 of ZASP). More problematic is the situation when the notes are distributed as photocopies among students, or even more so when the notes are uploaded to a freely accessible website. In the latter case, it is a communication to the public, which is considered to be the exclusive right of the copyright holder (e.g., the lecturer).²⁷ Recording lectures also means encroaching on copyright, as well as distributing a recording. Lectures may only be recorded if the lecturer agrees.

²⁴ Miha Trampuž (2000). Intelektualna lastnina: avtorska dela, ki nastanejo na univerzi. *Podjetje in delo*, 26, no. 6/7, p. 1283-1292.

²⁵ Ibidem.

²⁶ Article 9 of ZASP.

²⁷ Miha Trampuž (2000). Intelektualna lastnina: avtorska dela, ki nastanejo na univerzi. *Podjetje in delo*, 26, no. 6/7, p. 1283-1292.

Pedagogical exercises have a wide variety of content, which is why their definition of an author's work depends on the circumstances of the performance. For example, when exercises have elements of lectures, they are judged according to the same rules as lectures.²⁸ On the other hand, laboratory exercises are not supposed to be defined as authorial work.²⁹

So, the prerequisites for authorial work (at least as a rule) are met by lectures, seminars, textbooks, articles, reviews, expert opinions, research assignments, studies, and translation. However, rehearsals and exams can also mean copyrighted work in some instances.³⁰

6 Copyright Ownership in Employment

From copyright derives personality (moral copyright), property (material copyright), and other rights (other copyright).³¹ The ownership of the copyright in a copyrighted work that arises within the framework of an employment relationship, where both the employee and the employer contribute to the creation of copyright, is primarily a question of ownership of material copyrights and other copyrights.³² Copyright ownership in employment is regulated at the level of national law, which is why, for illustrative purposes, it will be highlighted below how the Slovenian ZASP addresses this issue.

In accordance with Article 14 of the ZASP, copyright always belongs to the author who created the copyrighted work. The author can only be a human person (not a corporate legal entity). A legal entity can be a copyright holder, but it cannot be an author. ZASP regulates copyrighted work from employment in articles 101 and 102. The rule set out in article 101 stipulates that when an employee creates a copyrighted work in the course of fulfilling his or her obligations or following the instructions of the employer, the material copyright and other rights of the author shall be transferred exclusively to the employer for a period of 10 years, unless otherwise

²⁸ Ibidem.

²⁹ Miha Trampuž, Branko Oman, Andrej Zupančič (1997). *Zakon o avtorskih in sorodnih pravicah (ZASP) s komentarjem*. Ljubljana: Gospodarski vestnik. p. 233.

³⁰ Elizabeta Zirnstein (2017). *Avtorska pravica iz delovnega razmerja na univerzi v Avtorska dela na univerzi* (ed. Martina Repas). Univerzitetna založba Univerze v Mariboru. p. 8.

³¹ Article 15 of ZASP.

³² Elizabeta Zirnstein (2017). *Avtorska pravica iz delovnega razmerja na univerzi v Avtorska dela na univerzi* (ed. Martina Repas). Univerzitetna založba Univerze v Mariboru. p. 3.

agreed. After this period, the rights return to the employee. Since the employer assigns the employee a payment based on the employment relationship, the rebuttable presumption of the transfer of material and other rights of the author in the copyrighted work applies. The employee and the employer may otherwise agree on the ownership of material and other rights in the contract (e.g., change the time period of ownership, agree on the content that will be the subject of the transfer, the amount of special compensation, etc.).³³

The importance of interpreting "according to the instructions of the employer" and "fulfilling one's obligations" is emphasised in order to place the creation of an author's work in an employment relationship. For scientific articles, scientific monographs, study materials, etc., the criterion "according to the instructions of the employer" is less applicable.³⁴ The very nature of scientific research almost conceptually excludes the possibility of giving instructions. Even if the instructions are shown in the form of basic ideas that encourage the creation of an author's work, they clash with the principle of academic freedom. Lectures, exercises, seminars and other direct pedagogical work of higher education teachers fall within the framework of "fulfilling one's obligations". As a result, higher education institutions have material copyrights over the mentioned forms of pedagogical work insofar as they are copyrighted works.³⁵

PowerPoint slides, slides, lecture handouts, hypothetical illustrative examples, exams, etc., created by higher education teachers for study purposes are considered borderline cases (this is a dilemma between placement between scientific research works - basic research and between the work obligation of higher education teachers, defined by acts of the higher education institution), where the ownership of copyright is conditioned by the circumstances of the creation of the copyrighted work. In particular, the relevant circumstances are whether preparing these works is a work obligation or whether the higher education teacher creates them on his own initiative. Since election to the title is a decision and not merely the meeting of formal conditions, it does not show the criteria for election to the title to be interpreted in the light of the "fulfilling of one's obligations" by the higher education teacher. Also,

³³ Ibidem, p. 3, 5, 6.

³⁴ Exceptions are computer programmes and databases.

³⁵ Elizabeta Zirnstein (2017). *Avtorska pravica iz delovnega razmerja na univerzi v Avtorska dela na univerzi* (ed. Martina Repas). Univerzitetna založba Univerze v Mariboru. p. 7, 8.

copyrighted works created in the framework of basic research cannot be placed in the criterion of "fulfilment of work obligations".³⁶

As students are not in an employment relationship, copyright ownership arrangements are out of the question. Even if they create a copyrighted work for the purposes of study obligations during their studies, they acquire full copyright. The same applies to final theses such as diploma theses, master's theses, or doctoral dissertations.³⁷ Supervising a higher education teacher in the final work or seminar work cannot mean co-authorship of the final work or seminar paper.³⁸

7 Exceptions to the Use of Copyright in Teaching or Research

Directive (EU) 2019/790, which Member States have to implement into national law by 7 June 2021 at the latest, amends Directive 2001/29/EC in certain areas. Both Directives are relevant, *inter alia*, to the field of copyright and related rights in education. Directive (EU) 2019/790 amends article 5 (3) (a) of Directive 2001/29/EC, which provides for one of the possibilities for the Member States to provide for exceptions and limitations to the rights provided for in articles 2 and 3 of this Directive (reproduction right and the right to communicate works to the public), as follows: "use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved, without prejudice to the exceptions and limitations provided for in Directive (EU) 2019/790". Except for minor changes resulting from the non-uniform translation of both directives,³⁹ the substantive change is subject to the annotation in Article 24 (2) (b) of Directive 2019/790 "without prejudice to the exceptions and limitations provided for in Directive (EU) 2019/790."

³⁶ *Ibidem*, p. 9, 10.

³⁷ *Ibidem*, p. 10 and Miha Trampuž, Branko Oman, Andrej Zupančič (1997). *Zakon o avtorskih in sorodnih pravicah (ZASP) s komentarjem*. Ljubljana: Gospodarski vestnik. p. 233.

³⁸ Elizabeta Zirnstein (2017). *Avtorska pravica iz delovnega razmerja na univerzi v Avtorska dela na univerzi* (ed. Martina Repas). Univerzitetna založba Univerze v Mariboru. p. 8.

³⁹ As far as we can compare English versions of article 24(2)(b) of Directive 2019/790 and article 5(3)(a) of Directive 2001/29/EC, the wording is identical, except the wording »without prejudice to the exceptions and limitations provided for in Directive (EU) 2019/790« in the wording of article 24(2)(b) of Directive 2019/790.

The exception provided for in Article 5 (3) (a) of Directive 2001/29/EC provides for the possibility of using all forms of copyright for illustrative purposes in teaching or scientific research, provided the source and author are indicated, for non-commercial purposes and to the extent necessary to achieve such a purpose. As this provision is optional, it is not necessary for Member States to introduce it. As a rule, the Member States that have implemented this provision have regulated it in two sets:

- Exceptions and limitations that appear in textbooks and compilations;
- Exceptions and restrictions for other forms of copyright used in education.⁴⁰

Implementation into national arrangements differs not only in introducing an exception or not but also in what exceptions are established in teaching and education. Exceptions and restrictions for other forms of copyrighted work relate to a range of possibilities for exploiting copyright content in teaching and education, from the use as well as the dissemination of texts to the performance of drama plays or film evenings.⁴¹

In Member States which have not opted to implement exemptions in education, in certain cases, copyrighted works for educational purposes may be used within the framework of citation rules. This exception can be even more useful in practice, as copyrighted work is allowed to be used, reworked, made available to the public, etc. Although on the other hand, the restrictions that apply for citation purposes (scope of use, etc.) must be taken into account.⁴²

As an example of the exception introduced under Article 5 (3) (a) of Directive 2001/29/EC, the provision of article 51 of ZASP, which states that, for the purpose of illustration, confrontation, or reference, it is permissible to cite excerpts or individually published fields of photography, fine arts, architecture, applied arts, industrial design, and cartography, provided the source and authorship are cited.

⁴⁰ Saša Krajnc (2017). Omejitve avtorske pravice za namene izobraževanja v Avtorska dela na univerzi (ed. Martina Repas). Univerzitetna založba Univerze v Mariboru. p. 38, 39.

⁴¹ Ibidem, p. 39, 42.

⁴² Ibidem, p. 44, 45.

Looking at the new Directive 2019/790, Member States will not have to adopt a new exemption under Article 5, provided that appropriate licensing is provided to allow the lawful use of copyrighted work.⁴³ The exception allows the sharing of copyrighted content only in closed electronic networks (e.g., intranet of educational institutions), which does not provide a basis for exchanging works outside the institution.⁴⁴

8 Conclusion

Respect of copyright encompasses all levels of education. Starting with preparing a group-work paper in primary school and all the way to the final work on study programmes. This topic also concerns teachers and lecturers in research and the pedagogical process. Their task is extremely crucial in mentoring the final and other works, where they meet and teach the authors about the respect of another author's copyrights under appropriate supervision. Due to the growing intertwining of education and information and communication technology tools and the ease of access to the works of another author, raising awareness of copyright protection is even more important. As a result, the work identifies aspects of copyright to which the author wanted to draw special attention. The main guideline is that the writer should use the rules of citation whenever he or she uses another author's work. The clearer and more detailed the citation rules are, the easier it will be for the writer to use another author's copyright. Finally, the role of EU law should be highlighted, where it is possible to identify quite a few possibilities for improving the current regulation about exceptions to the use of copyrighted works solely for the purpose of illustration in teaching or research.

References

- Bogataj Jančič, M., (2017). Velika pričakovanja in še večja razočaranja: Predlog direktive o avtorski pravici na digitalnem trgu v Avtorska dela na univerzi (ed. Repas, M.). Univerzitetna založba Univerze v Mariboru, 51-65.
- European Commission, Shaping Europe's digital future, The EU copyright legislation, accessible under: <https://digital-strategy.ec.europa.eu/en/policies/copyright-legislation> (25. 6. 2021).

⁴³ Ibidem, p. 46.

⁴⁴ Maja Bogataj Jančič (2017). Velika pričakovanja in še večja razočaranja: Predlog direktive o avtorski pravici na digitalnem trgu v Avtorska dela na univerzi (ed. Martina Repas). Univerzitetna založba Univerze v Mariboru. p. 56.

- European Union Intellectual Property Office Observatory – EUIPO, FAQs on Copyright, Pogosto zastavljena vprašanja o avtorskih pravicah, accessible under: <https://euiipo.europa.eu/ohimportal/sl/web/observatory/faqs-on-copyright-sl> (27. 6. 2021).
- Janez, Biblioblog, Plagiatorstvo in njegovo odkrivanje, accessible under: <https://www.biblioblog.si/2011/03/plagiatorstvo-in-njegovo-odkrivanje.html> (13. 6. 2021).
- Kanič, I., Knjižničarske novice, Plagiatorstvo in njegovo preprečevanje, accessible under: <http://old.nuk.uni-lj.si/knjiznicarskenovice/v2/podrobnostClanek.aspx?id=1202> (13. 6. 2021).
- Keresteš, T. (2017). Akademski plagiat v Avtorska dela na univerzi (ed. Repas, M.). Univerzitetna založba Univerze v Mariboru, 99-118.
- Krajnc, S. (2017). Omejitve avtorske pravice za namene izobraževanja v Avtorska dela na univerzi (ed. Repas, M.). Univerzitetna založba Univerze v Mariboru, 35-50.
- Ojsteršek, M., SlideServe, Preverjanje podobnosti vsebin v e-izobraževanju, accessible under: <https://www.slideserve.com/teagan-moss/preverjanje-podobnosti-vsebin-v-e-izobra-evanju> (13. 6. 2021).
- Tominc, P., Drozg, V., Ojsteršek, M., Samec, N., Korez, B., Kardum, D., Hržič, R. (2012). Preverjanje plagiatorstva na UM. Accessible under https://www.um.si/studij/splosno/Documents/Preverjanje%20plagiatorstva%20na%20UM%20-%20delovno%20gradivo_18_9_2012.pdf (13. 6. 2021).
- Trampuž, M. (2000). Intelektualna lastnina: avtorska dela, ki nastanejo na univerzi. *Podjetje in delo*, 26, št. 6/7, 1283-1292.
- Trampuž, M., Oman, B., Zupančič, A. (1997). Zakon o avtorskih in sorodnih pravicah (ZASP) s komentarjem. Ljubljana: Gospodarski vestnik.
- Univerzitetna knjižnica Maribor, Citiranje, accessible under: https://ukm.um.si/citiranje#_ftnref1 (18. 6. 2021).
- Weber-Wulff, D. (2014). False feathers: A Perspective on Academic Plagiarism. Springer. Zadeva C-161/17, Land Nordrhein-Westfalen proti Dirku Renckhoffu, z dne 7. avgusta 2018, ECLI:EU:C:2018:634.
- Zirnstein, E. (2017). Avtorska pravica iz delovnega razmerja na univerzi v Avtorska dela na univerzi (ed. Repas, M.). Univerzitetna založba Univerze v Mariboru, 1-14.

CYBERCRIME AND COMPUTER-RELATED OFFENCES

JAN STAJNKO, OSKAR PEČE

University of Maribor, Faculty of Law, Maribor, Slovenia
jan.stajnko@um.si, oskar.pece@student-um.si

Abstract The chapter describes crimes that users of online learning platforms usually encounter: the crime of illegal access to an information system, illegal interception, computer forgery, computer fraud, computer insults, and copyright infringements via IT systems. Special attention is given to regulating the aforementioned criminal acts in the Council of Europe Convention on Cybercrime. Some important pieces of legislation with which the EU harmonises this field are also mentioned, primarily Directive 2013/40/EU on attacks on information systems and Framework Decision 2008/913/PNZ on combating certain forms and expressions of racism and xenophobia by means of criminal law.

Keywords:

criminal law,
IT law,
cyberlaw,
cybercrime
convention,
EU criminal law,
European criminal
law

1 Introduction to Cybercrime

The term cybercrime covers crime connected to the globally connected space called cyberspace. Cybercrime can generally be defined as illegal conduct in which a computer or an information system is a tool or target of prohibited and harmful behaviour.¹ Here, it is important to divide such conduct into two types of cybercrime. Firstly, cybercrime is where the computer or information system is merely a tool (where the target is a person or organisation). Secondly, in crime, the information system itself is the target. The difference is that the first form of crime requires a lower level of knowledge regarding the use and operation of information systems and often represents a digital form of traditional crime (fraud, extortion, etc.), with the consequences occurring in the material and not the digital domain. The second type of cybercrime, where the information system is the target of illegal conduct, requires, as a rule, a higher level of knowledge about the operation and use of information systems. Moreover, consequences mainly arise in the digital domain (unauthorised entry into the information system, interception of data, disruption of the operation of information systems, etc.).²

As cybercrime is on the rise³, it is necessary to face these problems also in this manual. According to the authors, a list of crimes is discussed that users often encounter when using online learning platforms. These include illegal access to an information system, illegal interception, computer forgery, computer fraud, online defamation and hate speech, and copyright infringements via IT systems.

Users will typically encounter some of these crimes in the role of the victims, as the illegal attack will be directed against them or their information systems (and thus the legally protected goods, which they are the bearer of). In this sense, knowledge of the discussed offences makes sense so that users and professional staff at institutions are aware of them and know when it is appropriate to involve the police and the state prosecutor's office. On the other side, specific criminal acts are described, in which users typically find themselves in the role of the perpetrator (e.g., copyright infringement and online defamation and hate speech). The disclosure of these crimes

¹ M. Šepec, *Kibernetski kriminal*, 2018, pp. 7-8.

² K. Dashora, *Cyber Crime in the Society*, 2011, pp. 241-242.

³ N. Y. Conteh and M. D. Royer, *The rise in cybercrime and the dynamics of exploiting the human vulnerability factor*, 2016, p. 4.

makes sense in the light of the general preventive effect, i.e., as a warning to users to better understand when their behaviour may result even in criminal sanctions.

Although users will be able to find these crimes in national legislation, cybercrime is predominantly an international phenomenon. For this reason, definitions of criminal acts in national criminal law are generally aligned with the corresponding international legal framework. Within the framework of relevant international legislation, the Council of Europe Convention on Cybercrime ("Budapest Convention"), adopted on 23 November 2001 and entered into force on 1 July 2004, will be highlighted. Most European countries ratified it, but also countries outside of Europe such as the USA, Canada and Japan.⁴ The Convention contains a fundamental list of (cyber) crimes that should be criminalized by the signatory state.

Furthermore, based on paragraph 1 of Article 83 of the TFEU, the EU also has the competence to harmonize legislation in the field of computer crime. Therefore, the field of cybercrime and related crimes belongs to the so-called "Euro Crimes".⁵ Within the EU, this field is, therefore, additionally harmonised. It is necessary to highlight Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks on information systems and to replace Council Framework Decision 2005/222/JHA.⁶

2 Illegal Access to an Information System

The crime of illegal access to an information system is considered a core cybercrime. It is defined already in Article 2 of the Convention, which reflects the interests of organisations and individuals in the management and control of their information systems:⁷

"Each Party shall adopt such legislative and other measures as necessary to establish as criminal offences under its domestic law when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require

⁴ J. Clough, *A world of difference*, 2014, pp. 723-725.

⁵ K. Ambos, *European criminal law*, 2018, p.

⁶ For more on the Directive see L. Buono, *Fighting cybercrime between legal challenges and practical difficulties*, 2016, pp. 345-346.

⁷ Council of Europe, *Explanatory Report to the Convention on Cybercrime*, European Treaty Series - No. 185, 2001, p. 53.

that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system connected to another computer system."

Illegal access to an information system is an act of deliberate, unjustified and illegal entry into an information system or part of it, whereby the crime in question does not concern access to hardware, but access to data content stored in the information system. Unauthorised access to the information system can be carried out via a public or local communication network.

Unauthorised entry into the information system is not given in cases of merely sending e-mails with unwanted or potentially dangerous content. An actual entry into the information system is required, which means access to the data content of the information system.

To understand the problem of unauthorised access to an information system, it is necessary to clarify when such access is considered justified. Access to the information system is justified when the person who accesses the system is the owner of the system or accesses it based on a contractual relationship, authorisation of the owner or (written or verbal) consent of the user. When determining legitimate access, two types of entitlement must be distinguished, namely entitlement for general access and entitlement for access with a specific purpose. In the case of entitlement to general access, the beneficiary can also access the system for a purpose for which the entitlement was not explicitly granted. However, when the beneficiary only has the entitlement to access for a specific, precisely defined purpose (e.g., entitlement to use a computer to search for professional resources in databases), he may not access the information system and use it for another purpose (e.g., login to social networks).

Finally, the difference between unauthorised access to an information system and infringing on an information system should also be clarified. Infringing means any unauthorised access to an information system, which the perpetrator performs when he bypasses the system's security mechanisms or accesses the information system using technical means or another information system. Infringing is a special form of unauthorised access to an information system. Because the criminalisation of any unauthorised access to the information system could be too strict and non-life-

threatening today, the Convention allows the signatory countries to criminalise only that unauthorised access that corresponds to the concept of infringing information systems.⁸

3 Illegal Interception

Communication privacy is based on a reasonable expectation of privacy, protected in Article 8 of the European Convention on Human Rights.⁹ In order to protect the right to communication privacy, the Cybercrime Convention provides in Article 3:

»Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.«

Illegal interception (by technical means) refers to listening, monitoring or controlling the content of communications, obtaining the content of data, either directly, through access and use of a computer system, or indirectly, through the use of electronic eavesdropping or listening devices, where interception may also include recording. Technical means include technical devices attached to power lines, as well as devices for collecting and recording wireless communications. They include the use of software with direct access to the information system, as well as devices that read data indirectly, for example through the electromagnetic radiation of the devices (e.g. devices for catching and analysing the electromagnetic radiation of electric currents inside keyboards or keyloggers).¹⁰ The requirement to use technical means is a restrictive qualification, the purpose of which is to prevent excessive expansion of the scope of incrimination.¹¹ The described interception of computer data is, therefore often carried out without access to the information system, covertly and

⁸ M. Šepec, *Kibrenetski kriminal*, 2018, p. 61-70

⁹ *Ibid.*, p. 80

¹⁰ A. Završnik, *Napad na informacijski sistem*, 2018, pp. 693-694.

¹¹ Council of Europe, *Explanatory Report to the Convention on Cybercrime*, European Treaty Series - No. 185, 2001, p. 53.

without the victim's knowledge.¹² However, if the victim becomes aware that his or her computer data has been unlawfully intercepted (e.g., e-mail interception), it is helpful to immediately notify the competent authorities of the suspected criminal offence.

4 Computer-related Forgery

For the crime of forgery, it is essential that the perpetrator wants to create the appearance that a document was issued by a certain person, even though the statement in the document was not really made by this person. Therefore, the creation of a document which contains false or misleading information ("fake news" and the like) does not count as falsification of a document. Instead, the crime of forgery is the production of a document, in which the perpetrator forges a signature (and a stamp) and thereby creates a false impression that the document was issued by a certain person. For example, it is a criminal act of forgery if a person creates a false certificate of the result of a covid-19 test and thereby creates a false impression of the authenticity (credibility) of the issuer of the document. Changes to an existing authentic document, such as changing examination dates or other information on a medical certificate, are treated similarly. If the falsification of the document is done using the information system or if the electronic document is changed, such crime can be considered computer-related forgery.

Article 7 of the Convention on Cybercrime stipulates: »Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent before criminal liability attaches.«

¹² See M. Šepec, *Kibernetski kriminal*, 2018, p. 81

5 Computer-Related Fraud

In essence, fraud means taking advantage by causing harm or misleading another person.¹³ Misleading a person is usually related to the perpetrator's false claims about some factual circumstances. The essential element of this criminal act is also the fraudulent intention of the perpetrator - i.e., the intention to obtain a financial benefit or cause property damage. When fraudsters use an information system to commit fraud, such a crime can be considered computer-related fraud. As examples of computer fraud, criminal law theory cites fraudulent sales over the Internet (e.g., through an online platform such as eBay), cash advance fraud or Nigerian frauds (the fraudster allegedly needs an advance to later transfer inherited property and similar), wire fraud (e. g., persuading victims to invest in fictitious funds), fraudulent investments (various forms of fraud with fake websites) and identity theft (the perpetrator obtains financial gain by revealing the victim's identity).¹⁴ Computer fraud can be committed through the information system or against it (e. g., when the perpetrator deceives the information system so that it indirectly causes property damage to the injured party). A special form of cyberfraud is data manipulation, i.e., the change or deletion of data stored and published in the information system, with the aim of misleading another person.¹⁵

Article 8 of the Convention on Cybercrime stipulates: »Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right, the causing of a loss of property to another person by a) any input, alteration, deletion or suppression of computer data, b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or another person.«

6 Computer-Related Defamation and Hate Speech

Information systems can also serve communication that the legislator defines as inadmissible due to interference with a person's reputation (honour and good name). These legal goods are typically offended by crimes such as (computer-related)

¹³ Ibid., p. 163.

¹⁴ Ibid., pp. 166-168.

¹⁵ D. Shinder Littlejohn and M. Cross, *Scene of the Cybercrime*, 2008, p. 22.

defamation. Apart from crimes against reputation, cases of racist and xenophobic insults also ought to be tackled. The basis for criminalising such hate speech is not entirely left to national law. Instead, it can be found in international law, especially in the Additional Protocol to the Convention on Cybercrime, which deals with criminalising racist and xenophobic acts committed in computer systems and entered into force on 1 March 2006. Article 5 of the Additional Protocol stipulates:

»1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.

2) A Party may either a) require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule, or b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.«

The criminalisation of certain forms of hate speech, which is not only related to behaviour within cyberspace, is also harmonised in the EU member states by Council Framework Decision 2008/913/JHA of November 28, 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. At the international level (mainly in the EU), there are also initiatives to include members of the LGBT+ community as one of vulnerable groups, which ought to be protected from hate speech by national legislators by means of criminal law.¹⁶

7 Copyright Infringement via IT Systems or Digital Piracy

Offences related to copyright infringement through information systems have become one of the most widespread cybercrimes with the development of the Internet and the increasing use of digital media for the distribution of copyrighted

¹⁶ See European Commission, Union of Equality: LGBTIQ Equality Strategy 2020-2025, COM(2020) 698 final, 2020, p. 14.

works.¹⁷ Copyright infringement through information systems, or digital piracy, is the intentional and unjustified exploitation of an author's content through information systems, including the unjustified acquisition, reproduction, use and distribution of protected works (literary, photographic, musical, audio-visual, and other works¹⁸) as well as other forms of conduct which constitutes copyright infringement.¹⁹ The requirement to criminalise copyright infringement through information systems is set out in Article 10 of the Convention and establishes as a minimum standard of protection criminalisation of copyright infringements of commercial-scale (exploitation for commercial purposes²⁰), but does not exclude stricter national criminal provisions, which may also prohibit the unjustified exploitation of author's works in the private sphere or for non-commercial purposes.

In the context of the online educational environment, it is necessary to emphasise two forms of the described criminal offence, namely the creation and submission or publication of plagiarism (seminar papers, diploma theses or other contributions that can be uploaded to the online platform) and the use of protected photographs or images and other works in presentations, without obtaining appropriate permissions from the author. Audio or audio-video recordings of lectures are also controversial. Recording of lecturers on online platforms and their distribution (especially the sale of material obtained in this way) can therefore constitute a criminal offence of copyright infringement.

8 Conclusion

The legislative framework concerning cybercrime is one of the most dynamic and rapidly developing fields of criminal law. The reason for such rapid development is, on the one hand, connected to advancements in information and communications technology and, on the other hand, to the resourcefulness of cyberfraudsters and other cybercriminals. Hence, it is increasingly difficult for national lawgivers as well as international organisations to react to the ever-changing digital environment. The legislative framework regarding cybercrime is, therefore still associated with being full of grey and deregulated areas which need to be tackled in the future. Regardless,

¹⁷ M. Yar, K. F. Steinmetz, *Cybercrime and society*, 2019, p. 125.

¹⁸ Council of Europe, Explanatory Report to the Convention on Cybercrime, European Treaty Series - No. 185, 2001, p. 9.

¹⁹ See: M. Špec, *Kibrenetski kriminal*, 2018, p. 246

²⁰ See *ibid*, p. 249.

knowledge of fundamental cybercrime legislation (such as the Budapest Convention and EU legislation on cybercrime) is nonetheless useful for users of online learning platforms. When end users are equipped with such knowledge, they are able to timely report to the competent authorities that they were a victim of a cybercrime. What is more, expanding their knowledge solidifies their understanding of when their online conduct may be treated as illegal or even subject to criminal law sanctions.

Acknowledgements

We would like to thank Assoc. Prof. Dr. Miha Šepec from the University of Maribor for the review and suggestions for improvement of this chapter.

References

- Ambos, Kai, *European Criminal Law*. Cambridge University Press: Cambridge 2018.
- Buono, Laviero, *Fighting cybercrime between legal challenges and practical difficulties: EU and national approaches*. ERA Forum, 17(3), 2016, pp. 343-353.
- Clough, Jonathan, *A world of difference: the Budapest Convention on Cybercrime and the challenges of harmonisation*, Monash University Law Review, 40(3), 2014, pp. 698-736.
- Conteh, Nabie Y., and Malcolm D. Royer. "The rise in cybercrime and the dynamics of exploiting the human vulnerability factor." *International Journal of Computer*, 20 (1), 2016, pp. 1-12.
- Council of Europe, *Explanatory Report to the Convention on Cybercrime*, European Treaty Series - No. 185, 2001.
- European Commission, *Union of Equality: LGBTIQ Equality Strategy 2020-2025*, COM(2020) 698 final, 2020.
- Šepec, Miha, *Kibernetski kriminal: Kazniva dejanja in kazenskoppravna analiza*. Univerzitetna založba Univerze v Mariboru: Maribor 2018.
- Dashora, Kamini. *Cyber crime in the society: Problems and preventions*. Journal of Alternative Perspectives in the social sciences, 3(1), 2011, pp. 240-259.
- Shinder Littlejohn, Debra, and Cross, Michael, *Scene of the Cybercrime*, 2nd edition. Szngress Publishing: Burlington 2008.
- Yar, Majid, and Steinmetz, Kevin F., *Cybercrime and Society*, 3rd edition. SAGE: London, 2019.
- Završnik, Aleš, *Napad na informacijski sistem: 221. člen*, in: *Veliki znanstveni komentar posebnega dela kazenskega zakonika (KZ-1)*, 2. knjiga, Korošec, Damjan, Filipčič, Katja, and Zdolšek, Stojan (eds), *Zradni list Republike Slovenije: Ljubljana 2018*, pp. 676-708.

Moodle Basics – A User Guide

MARIUSZ GŁĄBOWSKI, JAKUB GRZELSKI,
KONRAD ŚNIATAŁA PAWEŁ ŚNIATAŁA, MICHAŁ WEISSENBERG

Introduction

This part of the book was developed as one of the main outputs of the **Cyber Security - Training Students and Scholars for the Challenges of Information and Communication Technologies in Research and Studies for Internationalisation (Cyber F-IT)** project. The authors aimed to bring together in one place the most important information on managing the various elements of the Moodle system. This part of the book was designed to facilitate the work of Moodle administrators (Part A) and teachers (Part B). Due to the different nature of the tasks and challenges faced by these groups, the document has been divided into dedicated parts.

Part A (User Guide for Admin) indicates the procedure for installing the Moodle service on a Linux Ubuntu distribution. This is followed by a list of the stages required to properly secure the entire service, create and manage users, and manage the server on which Moodle is running. The description as a whole allows administrators to be aware of all the tasks in each individual stage that lead to creating the Moodle platform and makes the implementation much more straightforward.

Part B (User Guide for Teachers) describes the most important areas of a teacher's daily work on the Moodle platform. The global management of the course template and its individual activities are presented. This allows the teacher to learn, step by step, about the administration of his/her course, the meaning of individual fields, and the possibilities of using various activities and resources. The first part describes the management of the course template, the choice of course views, and the settings for the entire course. This is followed by a discussion of the possibilities for managing individual topics within the course and a detailed description of all activities that can be added to the course and the procedure for adding them. The following section is devoted to the possibilities for creating student assessment. The types of questions that can be added to the course are described, corresponding examples, and a procedure for creating a test environment. The last section of Part B is devoted to backing the course up and restoring the course from an existing copy.

Part A

User Guide for Admin

1 Course Creation

This chapter describes the basic steps needed to create a Moodle on Ubuntu 20.04 Server.

1.1 Change Course Settings

Steps to install Moodle on Ubuntu 20.04 Server:

1. Connect to the server via SSH
2. Make sure that the server is up to date by using: `sudo apt update & sudo apt upgrade`
3. Install required MySQL and apache repositories: `sudo apt install apache2 MySQL-client MySQL-server PHP libapache2-mod-PHP`
4. Run secure MySQL installation: `sudo MySQL_secure_installation`. Remember to write down the password, you will need it in the next step

```
moodle@moodle:~$ sudo mysql_secure_installation
Securing the MySQL server deployment.
Connecting to MySQL using a blank password.

VALIDATE PASSWORD COMPONENT can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: yes

There are three levels of password validation policy:

LOW      Length >= 8
MEDIUM  Length >= 8, numeric, mixed case, and special characters
STRONG  Length >= 8, numeric, mixed case, special characters and dictionary file

Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 2
Please set the password for root here.

New password:
Re-enter new password:

Estimated strength of the password: 100
Do you wish to continue with the password provided?(Press y|Y for Yes, any other key for No) : yes
By default, a MySQL installation has an anonymous user,
allowing anyone to log into MySQL without having to have
a user account created for them. This is intended only for
testing, and to make the installation go a bit smoother.
You should remove them before moving into a production
environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : yes
Success.

Normally, root should only be allowed to connect from
'localhost'. This ensures that someone cannot guess at
the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : yes
Success.

By default, MySQL comes with a database named 'test' that
anyone can access. This is also intended only for testing,
and should be removed before moving into a production
environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : yes
- Dropping test database...
Success.
- Removing privileges on test database...
```

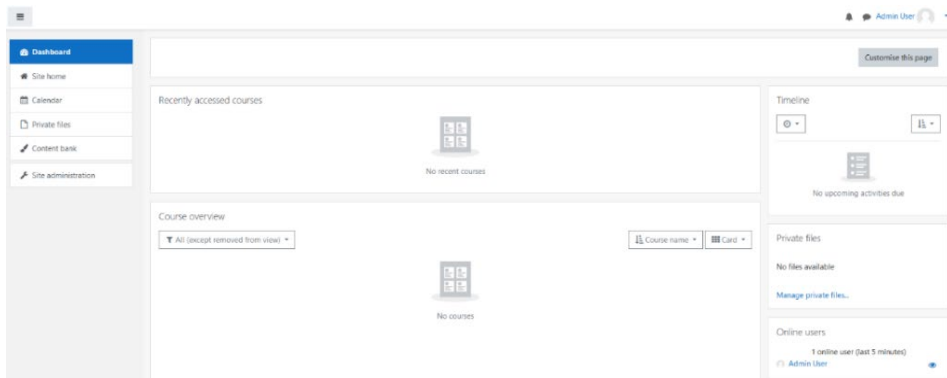
5. After installation, you will see the message: “All done!”
6. Install additional software: `sudo apt install graphviz aspell ghostscript clamav PHP7.4-pspell PHP7.4-curl PHP7.4-gd PHP7.4-intl PHP7.4-MySQL PHP7.4-xml PHP7.4-xmlrpc PHP7.4-ldap PHP7.4-zip PHP7.4-soap PHP7.4-mbstring`
7. Restart Apache so that the modules are loaded correctly: `sudo service apache2 restart`
8. Install Git because we will be using it to update Moodle: `sudo apt install git`
9. Change directory to /opt, we will put the Moodle core application code: `cd /opt`
10. Download Moodle code: `sudo git clone git://git.moodle.org/moodle.git`
11. Change directory to Moodle: `cd Moodle`
12. Retrieve a list of each branch available and tell git which branch to track or use: `sudo git branch -a; sudo git branch --track MOODLE_39_STABLE origin/MOODLE_39_STABLE`
13. Check Moodle version: `sudo git checkout MOODLE_39_STABLE`. You should see that branch is up to date
14. Copy the local repository to /var/www/html: `sudo cp -R /opt/moodle /var/www/html/`
15. Set proper permissions to files:
16. `sudo mkdir /var/moodledata`
17. `sudo chown -R www-data /var/moodledata`
18. `sudo chmod -R 777 /var/moodledata`
19. `sudo chmod -R 0755 /var/www/html/moodle`
20. Restart MySQL: `sudo service MySQL restart`
21. Create a database for Moodle and Moodle MySQL user. Use a password that you enter in d): `sudo MySQL -u root -p`
22. Create database: `CREATE DATABASE moodle DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;`
23. Create a user and password where it says „moodledude” and „passwordformoodledude” you should change to the username and password of your choosing: `create user 'moodledude'@'localhost' IDENTIFIED BY 'passwordformoodledude';` Remember to use a strong password, another way you will be informed to use a stronger password
24. Set permission to user:
`GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, CREATE TEMPORARY TABLES, DROP, INDEX, ALTER ON moodle.* TO 'moodledude'@'localhost';`

25. Exit database: quit;
26. Temporarily make the webroot writable by `sudo chmod -R 777 /var/www/html/moodle`
27. Go to `http://IP.ADDRESS.OF.SERVER/moodle` in your web browser and finish the installation
28. Set the language to English and click on “Next”
29. Change from `‘/var/www/moodledata’` to `‘/var/moodledata’`
30. Type set as: “Improved MySQL(native/MySQLi)”
31. Set a username and password like in 23. Other options set like on the screenshot:

Database host	<input type="text" value="localhost"/>
Database name	<input type="text" value="moodle"/>
Database user	<input type="text" value="moodledude"/>
Database password	<input type="text" value="zaq1@WSX123"/>
Tables prefix	<input type="text" value="mdl_"/>
Database port	<input type="text"/>
Unix socket	<input type="text"/>

[< Previous](#) [Next >](#)

32. Read and then accept conditions and click on “Continue”
33. Check if the server environment meets all minimum requirements.
34. Read installation summary, then click on “Continue”
35. Create a username and password for Moodle administrator. Set an email address and other optional fields. Then click on “Update profile”
36. Set Moodle Full site name, time zone, short name for the site, and no-replay address. Then click on “Save changes”
37. Now you can see Moodle dashboard



38. Set permission to file “config.PHP”: `sudo chmod -R 0755 /var/www/html/moodle`

1.2 Setting Password Policy for User

To set a password policy, follow these steps:

1. Go to “Site adm
2. inistration => Security => Site security settings”

At the bottom of the page, you will find password policy settings.

Set following variables:

- Password length: 8
- Digits: 1
- Lowercase letters: 1
- Uppercase letters: 1
- Non-alphanumeric characters: 1
- Log out after password change: Yes
- Remember username: optional

1.3 Register

The next step is to register your domain on Moodle.org, you will receive security messages. If you do not want to register your domain, you can follow security alerts on <http://moodle.org/security>.

2 Moodle Security

2.1 Securing Moodle From the Point of View of Network Addresses

If you know the IP address poll of your users, you can set a whitelist for IP addresses. Or the other way around, you can block addresses that should not have access to the Moodle website. You can do it in “Site administration => Security => IP blocker”.

moodle

[Dashboard](#) / [Site administration](#) / [Security](#) / [IP blocker](#)

IP blocker

Allowed list will be processed first
allowbeforeblock

Default: No

By default, entries in the blocked IPs list are matched first. If this option is enabled, entries in the allowed IPs list are processed before the blocked list.

Allowed IP list
allowedip

Default: Empty

Put every entry on one line. Valid entries are either full IP address (such as **192.168.10.1**) which matches a single host; or partial address (such as **192.168**) which matches any address starting with those numbers; or CIDR notation (such as **231.54.211.0/20**); or a range of IP addresses (such as **231.3.56.10-20**) where the range applies to the last part of the address. Text domain names (like 'example.com') are not supported. Blank lines, and text following a '#' character are ignored.

Blocked IP List
blockedip

2.2 Notification of Excessive Number of Password Attempts

Enable security notification in “Site administration => security => notification”. You will be notified if there are too many password attempts which may indicate a brute force attack.

moodle

Dashboard / Site administration / Security / Notifications

Notifications

Display login failures
displayloginfailures Default: No

This will display information to users about previous failed logins.

Email login failures to
notifyloginfailures

Default: Nobody

Send login failure notification messages to these selected users. This requires an internal logstore (eg Standard Logstore) to be enabled.

Threshold for email notifications
notifyloginthreshold Default: 10

If notifications about failed logins are active, how many failed login attempts by one user or one IP address is it worth notifying about?

- Display login failures: Yes
- Email login failures to <choose your username>
- The threshold to email notification: 10

2.3 HTTPS Security

Settings of HTTP security are in “Site administration => Security => HTTP security”. These settings should stay as they are by default.

Moodle

Dashboard / Site administration / Security / HTTP security

HTTP security

Secure cookies only
cookiesecure Default: Yes

If server is accepting only https connections it is recommended to enable sending of secure cookies. If enabled please make sure that web server is not accepting http:// or set up permanent redirection to https:// address and ideally send HSTS headers. When wwwroot address does not start with https:// this setting is ignored.

Only http cookies
cookiehttponly Default: No

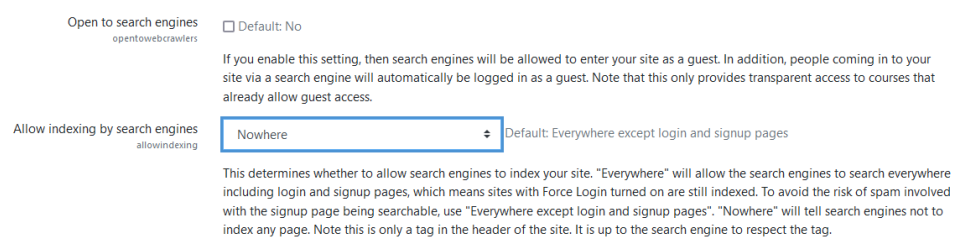
Enables new PHP 5.2.0 feature - browsers are instructed to send cookie with real http requests only, cookies should not be accessible by scripting languages. This is not supported in all browsers and it may not be fully compatible with current code. It helps to prevent some types of XSS attacks.

Allow frame embedding
allowframembedding Default: No

If enabled, this site may be embedded in a frame in a remote system, as recommended when using the 'Publish as LTI tool' enrolment plugin. Otherwise, it is recommended to leave frame embedding disabled for security reasons. Please note that for the mobile app this setting is ignored and frame embedding is always allowed.

2.4 Allow Indexing by Search Engines.

To allow indexing by search engines, you need to open – “Site administration => Security => Site security settings”.



The screenshot shows the 'Site security settings' page in Moodle. It features two main settings:

- Open to search engines** (opentowebcrawlers): A checkbox labeled 'Default: No' is currently unchecked. Below it, a text box explains: "If you enable this setting, then search engines will be allowed to enter your site as a guest. In addition, people coming in to your site via a search engine will automatically be logged in as a guest. Note that this only provides transparent access to courses that already allow guest access."
- Allow indexing by search engines** (allowindexing): A dropdown menu is set to 'Nowhere'. To its right, the text says 'Default: Everywhere except login and signup pages'. Below this, a text box explains: "This determines whether to allow search engines to index your site. 'Everywhere' will allow the search engines to search everywhere including login and signup pages, which means sites with Force Login turned on are still indexed. To avoid the risk of spam involved with the signup page being searchable, use 'Everywhere except login and signup pages'. 'Nowhere' will tell search engines not to index any page. Note this is only a tag in the header of the site. It is up to the search engine to respect the tag."

Option “Allow indexing by search engines” should be set as “Nowhere”.

2.5 Configure LDAP Authentication.

To integrate Lightweight Directory Access Protocol (LDAP) accounts with Moodle go to “Site administration => Plugins => Authentication => LDAP server”. LDAP defines a standard method for accessing and updating information in a local or remote directory (database) in the case of a client/server model. The protocol is optimised for reading, browsing and searching directories.

To configure LDAP authentication, you have to set:

1. Host URL – specify LDAP hostname or IP address
2. Distinguished name - If you want to use bind-user to search users. For example 'cn=ldapuser,ou=public,o=org'
3. Password: password to LDAP server
4. User type: Depended on LDAP settings
5. Context: List of contexts where users are located
6. Search subcontext: Yes
7. User attribute: Overrides the attribute used to name/search users. Usually, 'cn'
8. The rest of the fields can be left as they are by default. For., Data mapping (First name)” use „givenName”, „Data mapping (Surname)” – „sn”, „Data mapping (E-mail)” – „mail”

9. Now you can save settings by clicking on “Save changes” and then test settings by clicking on “Test settings”
10. To import users go to “Site administration => Server => Tasks => Scheduled tasks”. Find “LDAP users sync job”. Set the time when Moodle will synchronize users with LDAP. Also, you can run synchronisation manually from the server CLI (Command-Line Interface).

Moodle

[Dashboard](#) / [Site administration](#) / [Plugins](#) / [Authentication](#) / [Manage authentication](#)

Test authentication settings - LDAP server

Connecting to your LDAP server was successful

×

Continue

2.6 Support Contact

To set support contact information, go to “Site administration => Server => Support contact”. There is the possibility to set up a support email address and designate a special user responsible for support.

2.7 Secure Session

To secure sessions and limit the use of server resources, set a limit for the user session. You can do it in “Site administration => Server => Session handling”.

2.8 Efficiency

To increase efficiency, you can allocate more memory to physical resources on your server. The default value is set to 512MB. You can change it at “Site administration => Server => Performance”.

2.9 Notifications

By default, notifications about upgrades are on, and you should leave it as it is.

2.10 Quiz Hardening

Quiz hardening – limit access to quizzes with a password. To enable the option to set a password on a quiz, go to “Site administration => Plugins => Activity modules => Quiz” and enable “Require password”.

Quiz hardening – randomise question answers order. The default value of “Shuffle within questions” is enabled and can be changed in “Site administration => Plugins => Activity modules => Quiz”.

2.11 Brute Force Mitigation

The built-in mitigation to the brute force is located in “Site administration => Security => Site security settings => Account lockout threshold”. Here, we can set a threshold of the number of failed login attempts that result in account lockout. These settings should be considered because the attacker can lock the account and consequently prevent access to the actual account owners.

2.12 XSS/XSRF Mitigation

XSS consists of injecting malicious code into a web form or web address in order to perform a given operation. So there is a special function that can clean input data. This function can be enabled in “config.PHP” file on your server.

2.13 SQL Injection Mitigation

Changing settings relating to Structured Query Language (SQL) Injection attacks is impossible. The only mitigation is in the source code of Moodle, which cannot be edited. So, it is important to keep Moodle up to date.

2.14 Server Hardening

On the server which is running Moodle, only necessary services should be running. Useful tools to audit the server can be “Tiger” or “Lynis” (<https://github.com/CISOfy/lynis.git>). They can be used to generate a report about the machine.

2.15 Server Hardening – Local Firewall

The server should run a local firewall. The firewall should have ports needed for Moodle to function open properly. The necessary ports are 80, 443 (HTTP/HTTPS) and 9111 (chat). Example of access control list configuration:

```
sudo apt install iptables
sudo iptables -F
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A OUTPUT -o lo -j ACCEPT
sudo iptables -A INPUT -m state --state ESTABLISHED, RELATED -j
ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 9111 -j ACCEPT
```

To check settings, use:

```
sudo iptables -nL
```

And at the end, add a policy to drop anything else:

```
sudo iptables -P INPUT DROP
```

2.16 Logs Storage

Logs stored locally are located in “Site administration => Reports => Logs”. Logs can be filtered by participants/days/activities/actions sources/events. Logs are also stored in course backups if the proper option was chosen. Logs can also be exported to an external system, where they can be stored and analysed. Logs from Moodle and the server should be stored on a separate server. This can be done with “rsyslog”. Installation and configuration:

```
sudo apt install rsyslog
sudo systemctl start syslog
sudo vi /etc/rsyslog.conf
```

Then add the following line to the file:

```
*.*@@<adres_IP_serwera_syslog>:514
```

Now save the file and restart rsyslog:

```
sudo service rsyslog restart
```

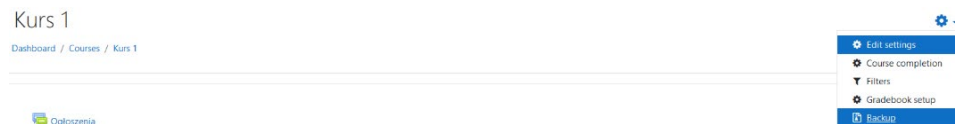
2.17 Logs Storage

The administrator can set verification of the age and location of the user by enabling the options in “Site administration => Users => Privacy and policies => Privacy settings”. By default, these settings allow you to configure the website according to the rules of the GDPR, allowing verification of the age of users. These settings should align with local policy (see Section “Privacy Settings”). It is also possible to enable/disable the display of a summary of stored private data. Next, in “Site administration => Users => Privacy and policies => Policy settings,” we can add URL to the data storage regulations, the website policy guide. In the “Site administration => Users => Privacy and policies => Plugin privacy registry”, there is a summary of the data collected by plugins installed on the platform. In “Site administration => Users => Permissions => User policies”, the administrator can change the visibility of profile elements of users.

3 Backup, Restore and Update

3.1 Creating a Backup Copy of a Course – Manual Mode

To create a manual backup copy of a course, you need to choose the course, click on the “gear” icon, and choose “backup”.



You will be redirected to a page with backup settings. There you can choose what data will be stored in the backup. You can jump to the final step or go for the next settings. On the second page, there are schema settings. In the third step, you can see a review of chosen settings and change the backup's filename. To finalfinalisebackup, click on "Perform backup". You should see the message "The backup file was successfully created." After this process, you can download the backup file and store it in a secure location.

3.2 Creating a Backup Copy of a Course – Automatic Mode

An automated backup schedule can be set in "Site administration => Courses => Backups => Automated backup setup."

Moodle

[Dashboard](#) / [Site administration](#) / [Courses](#) / [Backups](#) / [Automated backup setup](#)

Automated backup setup

Active
backup | backup_auto_active

Enabled Default: Disabled

Choose whether or not to do automated backups. If manual is selected automated backups will be possible only by through the automated backups CLI script. This can be done either manually on the command line or through cron.

Schedule
backup | backup_auto_weekdays

Sunday
 Monday
 Tuesday
 Wednesday
 Thursday
 Friday
 Saturday

Default: None

Choose which days of the week to perform automated backups.

Execute at
backup | backup_auto_hour

0 : 0 Default: 0:0

Choose what time automated backups should run at.

Automated backup storage
backup | backup_auto_storage

Course backup filearea Default: Course backup filearea

- Active: Enabled
- Schedule: Saturday (Copy should be performed when the server is not busy. Running the backup tool over all the courses can be processor-intensive, so you should not run it when there are many students on the server.)
- Execute at 00:00
- Automated backup storage: Course backup file area. Backups should also be stored on another server in case of failure.

- Maximum number of backups kept: 10
- Delete backups older than: depends on administrator choice
- Skip courses not modified since: 30 days

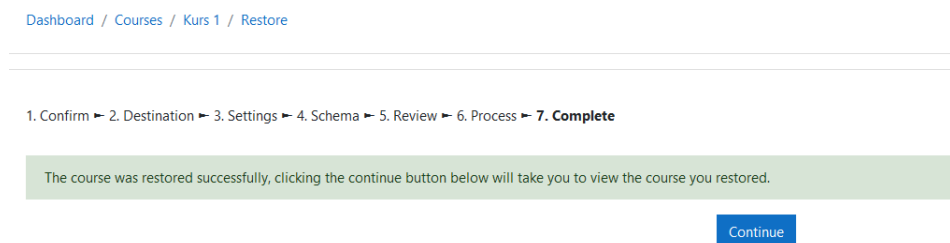
3.3 Course Restore – Manual Mode

To restore course data, you need to go to the chosen course, click on the “gear” icon, and then “restore”.



The course can be restored from a backup file stored on Moodle or from an external file.

After selecting the file, you will see a page with a summary. If the copy is correctly restored, you will see “The course was restored successfully, clicking the continue button below will take you to view the course you restored.”



3.4 Moodle Upgrade – Backup Important Data

Important data:

- Moodle software (everything in server/htdocs/moodle)
- Moodle uploaded files (server/moodledata)
- Moodle database (your Postgres or MySQL database dump)

- `cp moodle moodle.backup`
- `mv moodledata moodledata.backup`
- `MySQLdump -u username -p -C -Q -e -a moodle > moodle-backup.sql`

Put your site into maintenance mode to stop any non-administrator user from logging in. Then wait for any currently running cron processes to complete before proceeding.

Moodle

[Dashboard](#) / [Site administration](#) / [Server](#) / [Maintenance mode](#)

Maintenance mode

Maintenance mode
maintenance_enabled

Enable (Default: Disable)

Disable and other work

Optional maintenance message
maintenance_message

Default: Empty

Save changes

Check the requirements “Site administration => Server => Environment”

Moodle

[Dashboard](#) / [Site administration](#) / [Server](#) / [Environment](#)

[Update component](#)

Environment

Check how your server suits current and future installation requirements

Moodle version

Server checks

Name	Information	Report	Plugin	Status
moodle		❗ version 3.5 is required and you are running 3.9.9 (Build: 20210729)		OK
unicode		❗ must be installed and enabled		OK
database	mysql (8.0.26-0ubuntu0.20.04.2)	❗ version 5.6 is required and you are running 8.0.26.0.0.20.04.2		OK
php		❗ version 7.2.0 is required and you are running 7.4.3		OK
pcreunicode		❗ should be installed and enabled for best results		OK
php_extension	iconv	❗ must be installed and enabled		OK
php_extension	mbstring	❗ must be installed and enabled		OK

Download new files from Moodle and then unpack them:

```
tar xvzf moodle-1.1.tgz
```

Then copy the file:

```
cp moodle.backup/config.PHP moodle
cp -pr moodle.backup/theme/mytheme moodle/theme/mytheme
```

Now disable maintenance mode for everybody to be able to reaccess the Moodle.






























4 User Account Settings

4.1 Role Settings

Default roles and their permissions are in “Site administration => Users => Permissions => Define roles”.

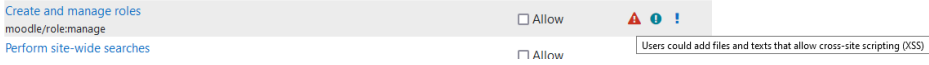
Moodle

[Dashboard](#) / [Site administration](#) / [Users](#) / [Permissions](#) / [Define roles](#)

Role 	Description	Short name	Edit				
Manage roles	Allow role assignments	Allow role overrides	Allow role switches	Allow role to view			
Manager	Managers can access courses and modify them, but usually do not participate in them.	manager	  				
Course creator	Course creators can create new courses.	coursecreator	   				
Teacher	Teachers can do anything within a course, including changing the activities and grading students.	editingteacher	   				
Non-editing teacher	Non-editing teachers can teach in courses and grade students, but may not alter activities.	teacher	   				
Student	Students generally have fewer privileges within a course.	student	   				
Guest	Guests have minimal privileges and usually can not enter text anywhere.	guest	  				
Authenticated user	All logged in users.	user	  				
Authenticated user on frontpage	All logged in users in the frontpage course.	frontpage	  				

[Add a new role](#)

Here you can create a role or edit an existing role. To edit the role, click on the “gear” icon on the right side. The roles and permissions should have been matched to the platform and users. If a permission is dangerous, there will be a red triangle on the right side with a description.



The granted rights should be set as low as possible while still allowing users to perform their tasks and properly use the platform.

4.2 Privacy Settings

Privacy settings are located in “Site administration => Users => Privacy settings”, and these are variables responsible for user privacy. By default, settings are customized to the chosen location. This means that when a new user selects the 'Create new account' button, they will be asked to enter their age and the country they are from.

Moodle

[Dashboard](#) / [Site administration](#) / [Users](#) / [Privacy and policies](#) / [Privacy settings](#)

Privacy settings

Digital age of consent verification
agedigitalconsentverification

No

Default: No

4.3 Authentication

Users can log in to the platform using local accounts created on the server or external authentication servers, such as the LDAP server. In “Site administration => Plugins => Authentication => Manage authentication” administrator can connect the external server to Moodle.

Moodle

[Dashboard](#) / [Site administration](#) / [Plugins](#) / [Authentication](#) / [Manage authentication](#)

Manage authentication

Available authentication plugins

Name	Users	Enable	Up/Down	Settings	Test settings	Uninstall
Manual accounts	3			Settings		
No login	0					
Email-based self-registration	0			Settings		Uninstall
CAS server (SSO)	0			Settings	Test settings	Uninstall
External database	0			Settings	Test settings	Uninstall
LDAP server	0			Settings	Test settings	
LTI	0					Uninstall
MNet authentication	0			Settings	Test settings	
No authentication	0			Settings		Uninstall
OAuth 2	0			Settings		Uninstall

To activate the pre-installed plugin, we need to first configure it by clicking on “Settings” and then try it by clicking on “Test settings”. If the test passes, we can enable the configuration by clicking on the “eye” icon.

4.4 Permission Summary

To display permissions of users go to “Site administration => Users => Accounts => Browse list of users”.

Moodle

Dashboard / Site administration / Users / Accounts / Browse list of users

2 Users

New filter

User full name

Show more...

Add filter

First name / Surname	Email address	City/town	Country	Last access	Edit
Admin Uzytkownik	jakub.			9 secs	
Jan Kowalski	jan.l			Never	

Add a new user

Users can be filtered by various filters, that are hidden under “Show more”. This way, accounts can be modified or removed from the platform. Only trusted administrators should have permissions to browsers users' accounts and modify or remove them.

4.5 Role For All Users

Under “Site administration => Users => Permissions => User policies”, it is possible to define default role for all users.

Moodle

Dashboard / Site administration / Users / Permissions / User policies

User policies

Role for visitors Default: Guest (guest)

Users who are not logged in to the site will be treated as if they have this role granted to them at the site context. Guest is almost always what you want here, but you might want to create roles that are less or more restrictive. Things like creating posts still require the user to log in properly.

Role for guest Default: Guest (guest)

This role is automatically assigned to the guest user. It is also temporarily assigned to not enrolled users that enter the course via guest enrolment plugin.

Default role for all users Default: Authenticated user (user)

All logged in users will be given the capabilities of the role you specify here, at the site level, in ADDITION to any other roles they may have been given. The default is the Authenticated user role. Note that this will not conflict with other roles they have unless you prohibit capabilities, it just ensures that all users have capabilities that are not assignable at the course level (eg post blog entries, manage own calendar, etc).

Creators' role in new courses Default: Teacher (editingteacher)

If the user does not already have the permission to manage the new course, the user is automatically enrolled using this role.

Restorers' role in courses Default: Teacher (editingteacher)

If the user does not already have the permission to manage the newly restored course, the user is automatically assigned this role and enrolled if necessary. Select "None" if you do not want restorers to be able to manage every restored course.

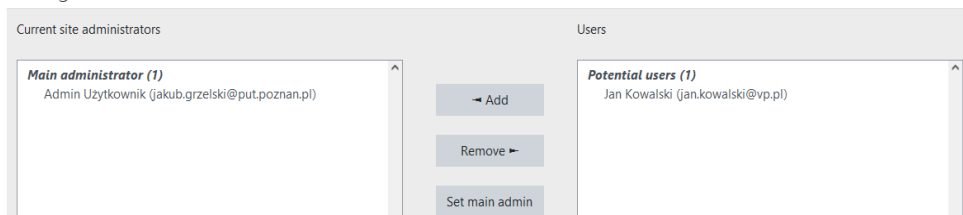
4.6 Adding Administrator

To add another administrator of Moodle go to “Site administrator => Users => Permissions => Site administrators”. In GUI we can add or remove administrators.

Moodle

[Dashboard](#) / [Site administration](#) / [Users](#) / [Permissions](#) / [Site administrators](#)

Manage site administrators



The screenshot shows the Moodle 'Manage site administrators' interface. It is divided into two main sections: 'Current site administrators' and 'Users'. In the 'Current site administrators' section, there is one entry: 'Main administrator (1)' with the email 'Admin Uzytkownik (jakub.grzelski@put.poznan.pl)'. In the 'Users' section, there is one entry: 'Potential users (1)' with the email 'Jan Kowalski (jan.kowalski@vp.pl)'. Between these two sections are three buttons: 'Add', 'Remove', and 'Set main admin'.

5 Server Settings

5.1 Developer and Testing Environment

The test environment should be an exact copy of the production site. It allows to test changes and evaluate platform behaviour. The administrator will be able to check the impact of changes on the server. The test environment should be accessible only from the internal network, with no access from the outside world, and isolated from the production server. The version of the development environment software should be the same as the version on the production server with the same config and plugins. Every change should be first tested on the development server. Testing the server is essential for continuous integration. After the test and positive results, the changes can be implemented on the production server.

5.2 Health Monitoring of the Server

Continuous monitoring of the server will allow you to notice irregularities in the work of the server. The server can be monitored by SNMP or special agents installed on the server. Health data collected by the monitoring server can be automatically

processed. Due to this, if the threshold is exceeded or events specified by the administrator occur, the administrator will be informed about the server state changes. Such events can be running out of disk space, CPU overheating, or loading on the network link to the server. Systems such as LibreNMS or Zabbix allow you to configure your triggers. Thanks to the long-term analysis of data collected by the system, the administrator will be able to configure alarms for events occurring in a server environment. If the trigger is activated, the action can be an e-mail or SMS. Active monitoring of the server's health can alert you about the strange behaviour of the server. It may mean that an unauthorized user has access to the server.

5.3 Automatic Vulnerability Search on the Server

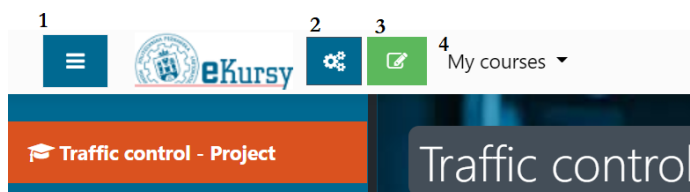
Opensource tools allow you to test the platform. Tools like “BurpSuite” can easily test the impact of attacks on path traversal, XSS, SQL Injection, XSFR, SSRF.

Part B

User Guide for Teachers

1 Course Homepage

The most important navigation elements on the course page:



1. List - access to the side panel
2. Gears - access to course management
3. Notepad - course editing mode
4. My courses - a list of the user's currently active courses

2 Course Creation.

This chapter describes the basic steps needed to create a course and how you can modify course elements, and how they affect the course, and how it is delivered.

2.1 Change Course Settings

This section covers the basic changes you can make to your course settings. To make changes, go to the subpage that allows you to change the course settings, available in the course settings panel.

2.1.1 Course Name

The name of the course should reflect the subject of the course. It is visible to users on the list of courses in which they participate and in the appropriate course category in the form of a link and in the navigation panel tab. After entering a given course, it is also displayed in the title bar of the web browser.

To rename a course, follow these steps:

1. Enable access to course management ("gears")
2. In the Course Settings pane, select Change Course Settings
3. In the "Full Course Name" field at the top of the page, enter a name for the course
4. Scroll to the bottom of the page and click on the Save and Display button

2.1.2 Course Visibility

Specify whether the course is to be visible to students after entering the appropriate subcategory and whether enrolled students are to see their course in their navigation panel. By default, a newly created course remains in the hidden state.

In a hidden state, the course remains visible to the course author and teachers assigned to it, and to people with administrative privileges. While it is hidden, students cannot access or see the course in the navigation pane even after they enrol in it.

To hide/show a course, follow these steps:

1. Enable access to course management ("gears")
2. In the Course Settings panel, select Change Course Settings
3. In the "Course Visibility" field, select the assumed option from the drop-down menu
4. Scroll to the bottom of the page and click on the Save and Display button

2.1.3 Course Format

Course format refers to the course layout. The course format can be set by following these steps:

1. Enable access to course management ("gears")
2. In the Course Settings pane, select Change Course Settings
3. In the "Course Format" pane, go to the "Format" drop-down menu and select one of the options
4. Scroll to the bottom of the page and click on the "Save and Display" button

There are several course formats, including:

- Weekly format - the format in which Moodle will create a separate section for each week of the course, including the dates in the header. The current week is automatically highlighted, and resources, activities can be placed in each section.
- Topics format (the default form of the course) - the format in which the course is divided into thematic sections with names specified by the teacher. Within each topic, you can include activities, resources and labels.
- Social format - a format focused on a social forum in which the facilitator can place any number of thematic discussions.
- Single activity format - the format in which the course is divided into only a single section in which the teacher can only place one activity.

Detailed descriptions are available at:

https://docs.moodle.org/310/en/Course_formats.

2.1.4 Course Start and End Date

The course start date affects how the course and logs are displayed, especially when selecting the weekly course format. The course end date is used to determine if the course should be included in your course list. After the end date has passed, the course is no longer displayed in the navigation block and is listed as past in the course overview on the student dashboards.

To set the start and end date of the course, follow these steps:

1. Enable access to course management ("gears")
2. In the Course Settings pane, select Change Course Settings
3. In the "General" panel, specify the start and end date of the course
4. Scroll to the bottom of the page and click on the Save and Display button

2.1.5 Course Description

The course description is divided into two sections: course summary and course image. To add a course description or image, follow these steps:

1. Enable access to course management ("gears")
2. In the Course Settings pane, select Change Course Settings
3. In the "Description" panel, complete the course summary and add a course image
4. Scroll to the bottom of the page and click on the Save and Display button

2.1.6 Course Summary

The summary will appear on the course list page. This field is searched when searching for a course and also appears in the course description block.

To add a course summary, follow these steps:

1. Enable access to course management ("gears")
2. In the Course Settings pane, select Change Course Setting
3. In the "Course Summary" panel, add a summary of the course
4. Scroll to the bottom of the page and click on the Save and Display button

2.1.7 Course Image

You can attach an image to your course summary. It will be available to anyone outside the course, as will the course name and summary. The course image is displayed as an icon in the list of available courses.

To place a course image, follow these steps:

1. Enable access to course management ("gears")
2. In the Course Settings pane, select Change Course Settings
3. In the "Course Image" panel, place an image file in one of the accepted formats: .gif, .jpeg, .png.
4. Scroll to the bottom of the page and click on the Save and Display button

2.1.8 Files and Uploads

It allows you to specify the maximum file size that can be sent by a student within the course. In the Moodle distribution used within the Cyber F-IT project the default is 500 MB.

To change the settings for the uploaded file size, follow these steps:

1. Enable access to course management ("gears")
2. In the Course Settings pane, select Change Course Settings
3. In the "Files and Upload" panel, select the maximum size of the uploaded file from the drop-down menu
4. Scroll to the bottom of the page and click on the Save and Display button

2.1.9 Groups

It allows you to change the course settings to divide users into groups. To change these settings, follow these steps:

1. Enable access to course management ("gears")
2. In the Course Settings pane, select Change Course Settings
3. In the "Groups" panel, you can change the selected options (described below)
4. Scroll to the bottom of the page and click on the Save and Display button

2.1.10 Group mode

In this section, you can define group mode at the course level using the drop-down menu. The options are "No Groups", "Separate Groups", and "Visible Groups". The selected setting will be the default group mode for all activities defined in this course. The group setting can affect what users see in the attendee list and with whom they can interact in the activities.

If you select "No groups", no user subgroups are created within the course, and activities are assigned by default to all participants.

When selecting "Separate Groups" in the course, each of the created groups sees only its group.

On the other hand, when selecting "Visible groups", the participants work within their subgroups but can see other groups in read only mode.

2.2 Course Management

This chapter describes the basic ways to manage users. The focus will be on the possible ways of enrolling students and teachers in the course, their data, and course roles. In addition, it will show how to create groups and assign students to them, as well as filter students on the list of participants. Additionally, the methods of contacting students and reports on their activity in the course will be discussed.

2.2.1 Course Enrollment Methods

Within the Moodle platform, there are several basic methods of adding students to a course.

Changes to the enrolment methods can be made as follows:

1. Enable access to course management ("gears")
2. In the User links panel, select Enrolment Methods
3. In the "Add enrolment method" field, select one of the options described below from the drop-down list

Within the Moodle platform, you can add the following user enrollment methods:

- Manual Enrolment – manual registration of users allows the teacher to assign users to the course on their own. There are two ways to do this.
 - After entering the "Enrolment methods" section (see above), in the list of saving methods, we find "Manual enrolment", and then in the modify column, select the "Save users" option.

Recording methods

Name	Users	Up/Down	Modifykuj
Manual saving	70	↓	 
Self-enrolment (Student)	0	↑ ↓	 
Auto enrolment	0	↑	 

Add a save method

- After enabling access to course management, in the User links panel, select the Participants tab (also available in the side panel). Then select the "Enrol users" button.

Participants



- Self-enrolment – enables users to enrol by themselves for the course by entering the password entered by the course creator. It is possible to define the time during which the user is allowed to enrol and the maximum number of users who can enrol in the course.
 - Enter your name for the saving method (any name).
 - Enter the access key to be made available to students.
 - Define the default role after accessing with a specific key; the default role is a student (description of roles available in the "course roles" section).
 - Set the start and end date of the period in which students can enrol (in the absence of a date, the student may enrol in the course at any time).
- Cohort sync – you add a group of users to the course. It is intended for student groups, academic year, etc. To add users via a cohort, follow these steps:
 - After enabling access to course management, in the User links panel, select the Participants tab (also available in the side panel). Then select the "Save users" button and in the "Select", a cohort section, select one of the possible cohorts from the drop-down menu (the Moodle platform administrators on the university side deal with assigning cohorts to specific groups of subjects).

2.2.2 User Data

To obtain information about students enrolled in the course, go to the Users subpage.

To do this, follow these steps:

1. Enable access to course management ("gears").
2. In the User Link panel, select Users.

The following fields are visible on the list of users:

- First name and last name
- Student index number
- E-mail
- Faculty
- Field of study
- Role in the course (for a description of the roles, see the Course roles subsection)
- Information about belonging to a group
- Date of last access to the course - the last time the student accessed the course
- Status

<input type="checkbox"/>	Name / Surname	Album number	Email	Department	Direction	Roles	Group	Last access to the course	Status
<input type="checkbox"/>	Michael					Course Author, Instructor, Coordinator	No groups	39 sec.	Active
<input type="checkbox"/>	Michael				Communications Technologies	Student	No groups	Never	Active
<input type="checkbox"/>	Maciej				ICT	Student	No groups	88 days	Active

In addition, by clicking on the name and surname of a specific student, you can get additional information, such as:

- Form of study.

- Type of study.
- Semester.
- Dean's group.
- Access to the full student profile..
- Add notes to the student.
- View specific student forum entries within the course.
- View the discussions started by the student in the course.



Message Add to contacts

User Details

Email

Direction

ICT

Department

Album number

Student number

Student Faculty

Student Direction

ICT

Current student semester

Dean's Group

Form of study

Type of study

Different

Full profile

Notes

My certificates

Forum Posts

Discussions started in the forums

Reports

Today's logs

All logs

Summary of the report

Full report

Statistics

Review of ratings

Administration

Log in as

Account Activity

Last access to the course

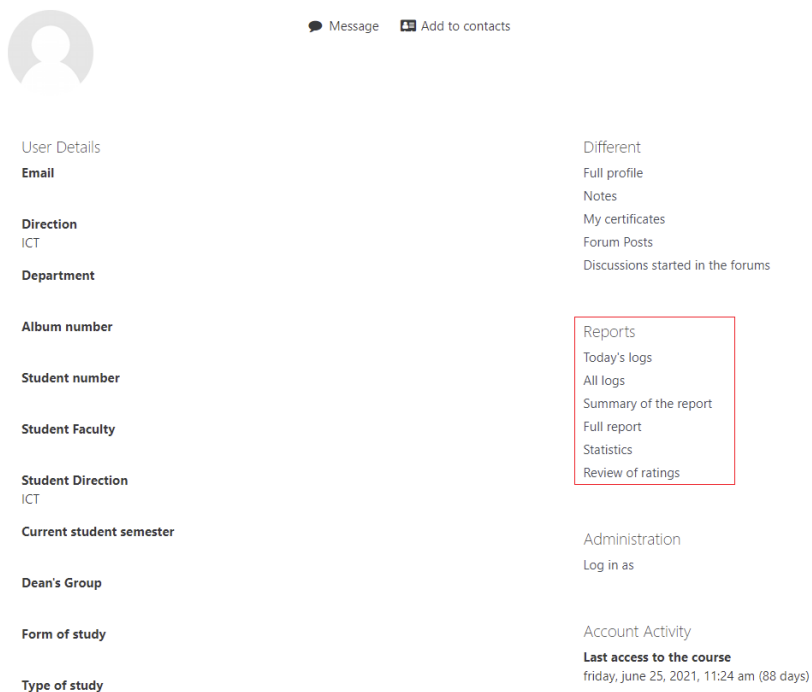
friday, june 25, 2021, 11:24 am (88 days)

Additionally, it is possible to generate several reports. This is described in the next subchapter for the user.

2.2.3 User Reports

To obtain user reports, follow these steps:

1. Enable access to course management ("gears").
2. In the User Link panel, select Users.
3. Then click on the name and surname of a specific student. Select one of the reports to be generated.



The screenshot displays a user profile interface. At the top left is a grey circular placeholder for a profile picture. To its right are two icons: a speech bubble labeled 'Message' and a plus sign labeled 'Add to contacts'. Below these are two columns of user details. The left column includes fields for 'Email', 'Direction' (ICT), 'Department', 'Album number', 'Student number', 'Student Faculty', 'Student Direction' (ICT), 'Current student semester', 'Dean's Group', 'Form of study', and 'Type of study'. The right column includes 'Different', 'Full profile', 'Notes', 'My certificates', 'Forum Posts', 'Discussions started in the forums', 'Administration', and 'Log in as'. A red rectangular box highlights the 'Reports' section, which contains the following items: 'Today's logs', 'All logs', 'Summary of the report', 'Full report', 'Statistics', and 'Review of ratings'. At the bottom right, under 'Account Activity', it shows 'Last access to the course' as 'friday, june 25, 2021, 11:24 am (88 days)'.

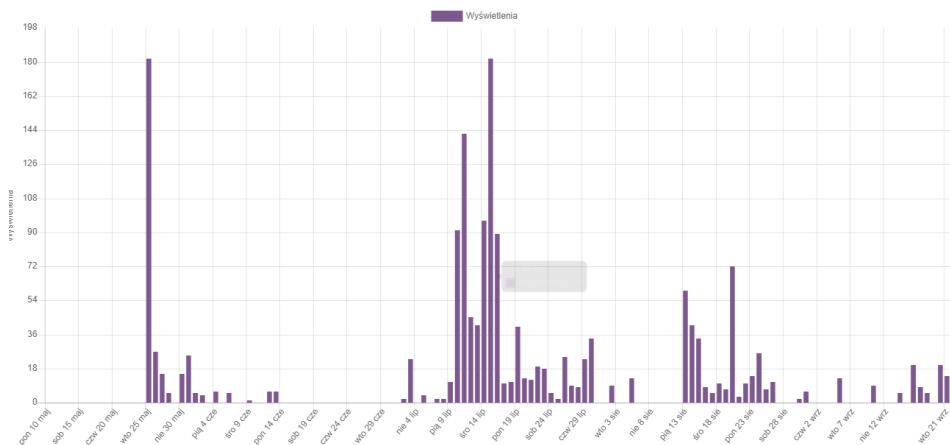
We can distinguish several types of reports:

- Today's logs - information about the user's activity on a given day within the course. The logs include:
 - Time - the exact date of the event.
 - Full name - name and surname of the student.
 - Applies to the user - in the case of an activity in the course, defines the activity to which the user has access.
 - Component - an activity to which the student has gained access.
 - Name of the event - the operation that the student performed in the activity.

- Description - a short description of the event.
- Source - definition of the browsing source, e.g., web in the case of a website.
- IP address - the address from which the access was obtained.

Time	Full name	Applies to the user	Event context	Ingredient	Event name	Description	Source	IP address
21 september 2021, 12:25	Michael	Michael	Course: Artificial Intelligence 2021	System	User profile displayed	The user with id '6701' viewed the profile for the user with id '6701' in the course with id '14444'.	web	

- All logs - information about users' activity within the course throughout its duration. It contains the same data as today's log report and activity graph.



- Report summary - information about the user's activity within specific topics, such as the number of views on individual activities, obtained ratings in the activities.

AI Course

- Announcements -
- Link to the list of courses 1 insights wednesday, june 2, 2021, 11:49 am (111 days)
- Consultation -
- Job fair 1 insights wednesday, june 2, 2021, 11:49 am (111 days)
- Courses in September - survey No response

Experimental data set

- Experimental Data Set -

Lab Guide

- Python Lab Guide -
- Machine Learning Lab Guide -
- Machine Learning - solution of tasks 1, 2 and 3 -

- Full report - an extension of the report summary with attached files, and comments about the tasks.
- Statistics - a collection of information about the number of views, entries, and all activities in the course, broken down by month.

End of period	Display	Entries	All activities
31 august 2021	184	30	214
31 july 2021	590	117	707
30 june 2021	12	0	12

2.2.4 Course Roles

In the course, we can define several basic roles that can be assigned to users:

- Site administrator - By default, the course administrator is authorized to perform all operations in the course.
- Course creator - can create and manage a course by adding users, blocks, and changes course settings. This role is often associated with the person teaching a given course. Still, it can also be assigned to the tutor of a given field of study or the curriculum coordinator.
- Teacher - by default, the teacher within the course has the right to add and change blocks within the course, add activities and users. Additionally, the teacher can change the role of users (in terms of students and teachers without editing rights).
- Non-editing teacher - has the right to view and rate student work but does not have the right to change or add new resources in the course. Additionally, you can restrict non-editing teacher access to specific groups within the course.
- Student – has the right to participate in the course and has access to the course resources but may not edit the course or view the grading log. You can also restrict student access to specific resources by their name, identification number (e.g., index number), specifically assigned group, etc.

2.2.5 Group Creation and Administration

Entering groups in a course allows you to filter actions and grades for specific user groups and grant non-editing access to teachers and students to specific activities, resources, and topic sections.

- Group levels
 - Course level - selecting this level assigns group mode as the default mode for all added activities within the course. To enable this level, follow the steps described in the Course Creation chapter, subchapter Change Course Settings - Groups.
 - Activity level - for each activity that supports group mode, it can be assigned independently. The assignment of group mode to a single activity has been described individually for each activity.

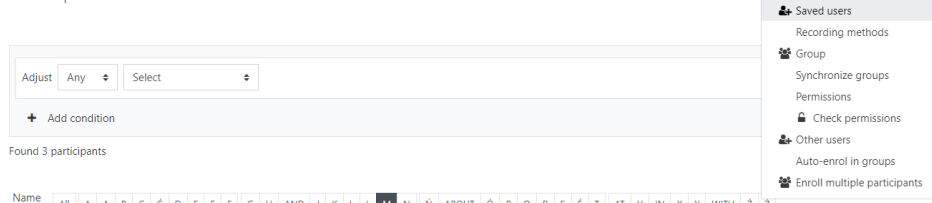
To create a new group, follow these steps:

1. Enable access to course management ("gears")
2. In the User Link panel, select Groups
3. Select Create Group

Another way to access groups is to follow these steps:

1. Enable access to course management ("gears")
2. In the User Link panel, select Users
3. Select the group field from the drop-down menu with additional options
4. Select Create Group

Participants



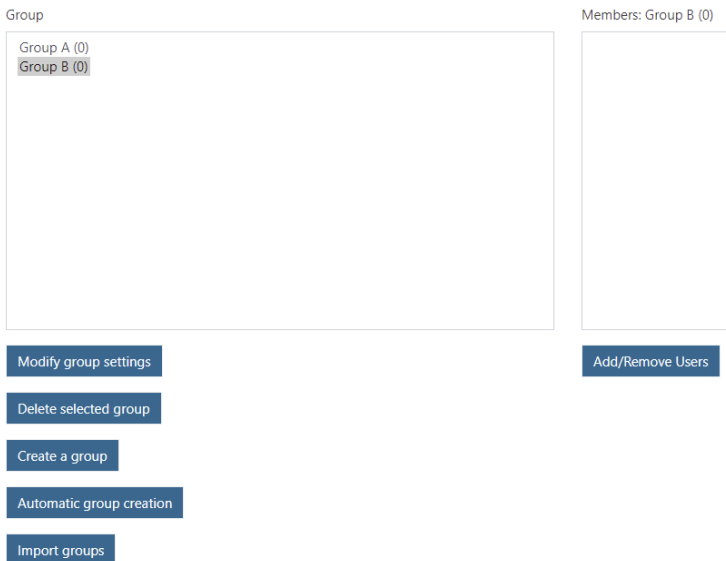
The screenshot shows the 'Participants' page in Moodle. At the top right, there is a gear icon for settings. Below it is a dropdown menu with the following options: Saved users, Recording methods, Group, Synchronize groups, Permissions, Check permissions, Other users, Auto-enrol in groups, and Enroll multiple participants. The main content area has a filter bar with 'Adjust Any' and 'Select' dropdowns, and an 'Add condition' button. Below the filter bar, it says 'Found 3 participants'. At the bottom, there is a table with a 'Name' column and a row of letters: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z.

When creating a group, you can specify, among other things, the following parameters:

- Group name - the name visible to the teacher in all activities for which group operations can be performed.
- Group information - optional information about the group
- Access key to the group in the case of individual registration by course participants.
- Messages to the group - It allows members of the group to send messages to other participants.

To add new users to the previously created group, follow these steps:

1. Enable access to course management ("gears")
2. In the User Link panel, select Groups
3. On the list of groups, select the group to which you want to add students
4. Then click on the Add / Remove Users button

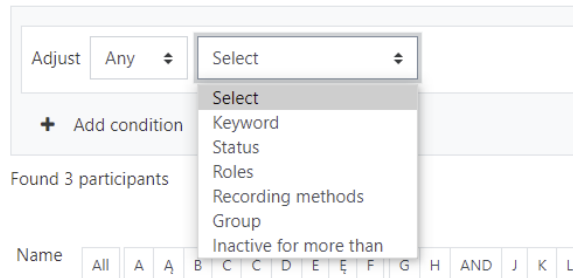


5. Select the student who is to be added to or removed from the group and select the appropriate button

2.2.6 Filtering the List of Users

To filter the user list, follow these steps:

1. Enable access to course management ("gears")
2. In the User Link panel, select Users
3. At the top of the page, select the filtering option:



3.1 In the first field, define how the filtering conditions must be met:

- None – no condition has to be met.
- Any – Any of the filtering conditions must be met.
- All – All of the filtering conditions must be met.

3.2 In the second field, define which filtering method should be used, you can choose from:

- Keyword - a keyword that must be in one of the columns with user information.
- Status - active/inactive.
- Roles - one of the roles described in the section "Course roles".
- Enrolment methods - manual/standalone.
- Groups - one of the groups created as part of the course.
- Inactive for longer than – the definition of days since the last student activity in the course.

2.2.7 Contact With Users

To send a message to a specific user, the following steps can be performed:

1. Enable access to course management ("gears")
2. In the User Link panel, select Users
3. Select the checkbox next to the student to whom the message is to be sent
4. At the bottom of the page, from the "With selected users" drop-down menu, select the "Send Message" option

To send the message to all users, you can follow these steps:

1. Enable access to course management ("gears")
2. In the User Link panel, select Users
3. Select all users on the list of users by checking the checkbox in front of the first and last name field, or using the button at the bottom of the page "Select all users"
4. At the bottom of the page, from the "With selected users" drop-down menu, select the "Send message" option

To send a message to a specific group of users, you can follow these steps:

1. Enable access to course management ("gears")
2. In the User Link panel, select Users
3. Filter users by groups and select a specific group following the instructions described in the section "Filtering the list of users"
4. Select all users on the list of users by checking the checkbox in front of the first and last name field, or using the button at the bottom of the page "Select all users"
5. At the bottom of the page, from the "With selected users" drop-down menu, select the "Send message" option





2.2.8 Activity Reports

The course activity report is available to the administrator, course creator, teacher, and teacher without editing rights. As part of the overall activity report, you can see the number of views for each activity and the resource within the course.

To generate an activity report:

1. Enable access to course management ("gears")
2. In the User Link panel, select View Course Activity Reports

Lab Guide

 Python Lab Guide	68 showing by 41 users	thursday, september 2, 2021, 3:02 pm (18 days 21 hours)
 Machine Learning Lab Guide	65 displayed by 32 users	thursday, september 2, 2021, 3:02 pm (18 days 21 hours)
 Machine Learning - solution of tasks 1, 2 and 3	91 showing by 38 users	thursday, september 2, 2021, 3:02 pm (18 days 21 hours)
 Machine Learning - solution of tasks 4, 5 and 6	27 showing by 19 users	thursday, september 2, 2021, 3:02 pm (18 days 21 hours)

It is also possible to generate a detailed report for each course participant. Information on the method of generating reports for individual users is included in the User Data subsection.

3 Topic Management

This chapter describes the basic mechanisms for managing topics within the course. The focus will be on creating the topic and managing its settings, as well as the activities and resources that can be placed inside the course.

3.1 Topic Editing

This section covers the basics of the topics for the courses on the platform. To add a new topic, please complete the following steps:

1. Access to the course editing mode ("notepad") must be enabled on the course website
2. At the bottom of the page, we find the "add topic"
3. We define the number of added topics in the "Number of sections" field

To edit a course, follow these steps:

1. Access to the course editing mode ("notepad") must be enabled
2. Next to the name of the course on the right, select the drop-down menu
3. We choose one of the options:

- Edit topic – switch to the topic editing mode.
- Highlight – the topic on the page is highlighted with a frame.
- Show topic/Hide topic – setting the visibility of the topic from the student's point of view.
- Delete Topic – delete the topic and all the activities created in it.

As part of editing a topic, you can perform the following actions:

- Post a topic - visible at the top of the section.
- Add an abstract - the description of the topic is visible under the topic name.
- Access limitation - you specify the activity availability only for individual users; you can choose from the following options:
 - Cohort - limited to a specific student cohort only..
 - Complete an Activity - require other activities to be completed before access.
 - Date - you define access only at a specific time.
 - Assessment - the requirement to obtain an appropriate grade (as a percentage) for another activity.
 - Password - requires a password to access the resource.
 - Roles - you define access based on the user's role in the course.
 - Restriction set - you specify a set of restrictions that must be met before being granted access.

In addition, within a specific topic, you can add activities and resources that are described in detail in the following subsections.

3.2 Forums and Chats

This section covers the basic community activities that can be added as part of the course.

As part of social activities, the following can be distinguished:

- Forum - the forum you add threads and comments, both for teachers and students. As part of the forum entries, multimedia files can be placed.
- Chat - This allows course participants to discuss in real time.

3.2.1 Forums

There are 5 types of forums within the moodle platform:

- Q&A forum - Instead of initiating a discussion, participants ask a question in the initial discussion post. Students may respond but will not see other Students' answers to a question in the discussion until they respond in the same discussion.
- Standard forum for general use - an open forum where anyone can start a new topic at any time; this is the best general-purpose forum.
- Everyone sends a discussion topic - each person can post exactly a new discussion topic (although anyone can reply to it); this is useful when you want each student to start a discussion on, say, their thoughts for the week, and everyone else to respond to them.
- Single Discussion - A single-page discussion of one topic that is useful for short, focused discussions (cannot be used with separate groups).
- Standard forum displayed like a blog.

To add a forum, follow these steps:

1. Access to the course editing mode ("notepad") must be enabled on the course website.
2. As part of the topic in which the forum is to be placed, click on "Add activity or resource".
3. In the list of activities, find a forum and then click on the activity icon.

Basic settings when creating a forum:

- Name - Define the name displayed on the course page.
- Description - optional additional description of the activity displayed on the course website.

- Type - you choose one of the options described above.
- Availability - allows you to set the availability time of the forum for students.
- Attachments and word counting - you specify the maximum size and number of attachments placed within the forum and specify whether words should be counted within forum posts.
- Subscription and observation - you define the method of subscribing and observing the forum. We can distinguish:
 - Subscription (in the case of subscribing to the forum, users receive an e-mail with content of any new posts on the forum):
 - Optional subscription - course participants can decide on their own to subscribe to the forum.
 - Force Subscription - All course participants are subscribed to the forum and cannot change it.
 - Automatic subscription - after creating a forum, all course participants are automatically assigned as subscribers to the forum; however, they can change it.
 - Subscription disabled - course participants cannot subscribe to the forum.
 - Observation (in the case of observation, participants have the option to see which posts on the forum they have not yet seen by highlighting them):
 - Optional - allow students to choose whether they want new messages to be highlighted.
 - Off - all new posts are automatically highlighted.
- Blocking - you define whether forum discussions should be blocked after a certain period with no new entries.
- The threshold for entries to be blocked.
- Grading - It is possible to define the types of attendance with points, scale, and none, which means no attendance scores. Additionally, you can assign attendance grades to the appropriate grade category and define the attendance credit threshold.
- Standard module options - you determine the availability (whether the activity should be visible to students), with an option of adding an ID number and a group mode in the case of many groups.

- Access limitation - you specify the activity availability only for individual users; you can choose from the following options:
 - Cohort - limited to a specific student cohort only.
 - Complete an Activity - require another activity to be completed before access.
 - Date - you define access only at a specific time.
 - Assessment - the requirement to obtain an appropriate grade (as a percentage) for another activity.
 - Password - requires a password to access the resource.
 - Roles - you define access based on the user's role in the course.
 - Restriction set - you specify a set of restrictions that must be met before being granted access.
- Activity Completion - you define how you track your completion and expectations for an activity by a deadline.

3.2.2 Chats

To add a chat, follow these steps:

1. Access to the course editing mode ("notepad") must be enabled on the course website
2. As part of the topic in which the forum is to be placed, click on "Add activity or resource"
3. In the list of activities, find a "chat" and then click on the activity icon

Basic settings when creating a chat:

- Name - Define the name displayed on the course page.
- Description - optional additional description of the activity displayed on the course website.
- Chat sessions - you define the following chat parameters:
 - Next chat time - you define the date of the next chat session; this date is automatically placed in the participant's calendar.

- Repeat/publish session times - allows you to schedule new chat sessions automatically; there are four options to choose from:
 - do not show session times - after selecting this option, the exact chat hours are not set, and chat users can use it for the entire duration of the course.
 - do not repeat - after selecting this option, only the time of the next meeting will be published in the form of a chat.
 - every day at the same time - when selected, the chat is scheduled every day at the same time.
 - weekly at the same time - when selected, the chat is scheduled at the same time every week.
- Keep past sessions - you define for how many days the chat record should be kept.
- Anyone can view past sessions - you specify whether all course participants can view the record of past chat sessions (teachers can always view past sessions, this setting applies to students).
- Standard module options - you determine the availability (whether the activity should be visible to students), optionally adding an id number and a group mode in the case of many groups.
- Access limitation - you specify the activity availability only for individual users; you can choose from the following options:
 - Cohort - limited to a specific student cohort only.
 - Complete an Activity - require another activity to be completed before access.
 - Date - you define access only at a specific time.
 - Assessment - the requirement to obtain an appropriate grade (as a percentage) for another activity.
 - Password - requires a password to access the resource.
 - Roles - you define access based on the user's role in the course.
 - Restriction set - you specify a set of restrictions that must be met before being granted access.
- Activity Completion - you define how you track your completion and expectations for an activity completion date.

3.3 Attendance

Attendance activity allows you to keep a list of student attendance during classes. It allows you to set class dates, assign appropriate groups to dates, etc.

To create an attendance activity, follow these steps:

1. Access to the course editing mode ("notepad") must be enabled on the course website
2. As part of the topic in which the forum is to be placed, click on "Add activity or resource"
3. In the list of activities, find the attendance and then click on the activity icon

Basic activity settings:

- Name - you define the name displayed on the course page.
- Description - optional additional description of the activity displayed on the course website.
- Grade - it is possible to define attendance grades in a point, scale, and none, which means no attendance scores. Additionally, you can assign attendance grades to the appropriate grade category and define the attendance credit threshold.
- Standard module options - you determine the availability (whether the activity should be visible to students), optionally adding an id number and a group mode in the case of many groups.
- Access limitation – you specify the activity availability only for individual users; you can choose from the following options:
 - Cohort - limited to a specific student cohort only.
 - Complete an Activity - requires another activity to be completed before access.
 - Date - you define access only at a specific time.
 - Assessment - the requirement to obtain an appropriate grade (as a percentage) for another activity.
 - Password - requires a password to access the resource.
 - Roles - you define access based on the user's role in the course.

- Restriction set - you specify a set of restrictions that must be met before being granted access.
- Activity Completion - you define how you track your completion and expectations for an activity completion date.

After creating the attendance activity, you get access to the activity panel. Inside the panel, the following options are available on specific tabs:

#	Date	Time	Type	Description	Actions
1	wed, 22 sep 2021	09 - 11	Group: TM18	Regular classes	▶ ⌂ 🗑

- Sessions - access to the view of created sessions.
- Add session - you add a new session:
 - Session type - shared or group in case of creating groups in the course.
 - Session date - define the date of the meeting.
 - Time - meeting time.
 - Description - optional description.
 - Add multiple sessions - allows you to create multiple repeating sessions; it is especially useful for repeated activities.
 - Registration by the student - enabling the student to independently mark his or her presence in the tab.
- Report - reports for visible sessions.
- Export - allows you to export session information to a file in one of three formats (Excel (.xlsx), OpenOffice (.ods), text file (.txt)).
- Status set - you define the presence statuses and the points earned for them. By default, four statuses are set: P - present, L - late, E - excused, and A - absent. In addition, you can define the time during which a particular option is available to the student (e.g. specifying that attendance can only be checked for the first 5 minutes, then the late option is available). Additionally, you can choose an option set by default if the student selects no option.

3.4 Activities and Resources

This section describes the basic activities and resources to improve and enhance the quality of delivering courses for students.

3.4.1 Labels, Links, and Files

The section covers the basics of applying, placing, and editing labels, links, and files.

3.4.1.1 Labels

The label can be used to create the course structure and spacing within individual topics (a division of the topic into sections). As part of this course resource, the tutor has the option of both plain text and multimedia (images, audio/video recordings) and links. In particular, the job of the labels is to improve the appearance of the topic and separate sections.

To create a label inside a topic, follow these steps:

1. Access to the course editing mode ("notepad") must be enabled on the course website.
2. As part of the topic in which the forum is to be placed, click on "Add activity or resource."
3. In the list of activities, find the label and then click on the resource icon.

Basic resource settings:

- Label text - you enter the label text (text, multimedia, link) that will be displayed on the course page.
- Standard module options - you determine the availability (whether the activity should be visible to students), optionally adding an id number and a group mode in the case of many groups.
- Access limitation – you specify the activity availability only for individual users; you can choose from the following options:
 - Cohort - limited to a specific student cohort only.

- Complete an Activity - requires other activity to be completed before access.
- Date - you define access only at a specific time.
- Assessment - the requirement to obtain an appropriate grade (as a percentage) for another activity.
- Password - requires a password to access the resource.
- Roles - you define access based on the user's role in the course.
- Restriction set - you specify a set of restrictions that must be met before being granted access.

3.4.1.2 Links

The URL may be used as part of the course to provide course participants with a link to external resources that cannot be included in the course.

To add a link inside a topic, follow these steps:

1. Access to the course editing mode ("notepad") must be enabled on the course website.
2. Under the topic where the link is to be placed, click on "Add activity or resource."
3. In the list of activities, find the URL address and click on the resource icon.

Basic resource settings:

- Name - link name, text visible to course participants.
- External URL - www address to which the link should be redirected.
- Description - description of the link visible to course participants.
- Appearance - you define how the reference page should be displayed; there are four options:
 - Automatically.
 - Embedded - the referenced website is embedded within the Moodle platform, leaving the course header and blocks.

- Open - you are directly redirected to the website within the current browser tab.
- In the pop-up window – the website opens within a new browser window.
- Changing the URL address - transfers internal information from moodle course such as course data (id, course name, etc.), and user data (id, first name, e-mail, etc.) to the URL.
- Standard module options - you determine the availability (whether the activity should be visible to students), optionally adding an id number and a group mode in the case of many groups.
- Access limitation - you specify the activity availability only for individual users; you can choose from the following options:
 - Cohort - limited to a specific student cohort only.
 - Complete an Activity - requires another activity to be completed before access.
 - Date - you define access only at a specific time.
 - Assessment - the requirement to obtain an appropriate grade (as a percentage) for another activity.
 - Password - requires a password to access the resource.
 - Roles - you define access based on the user's role in the course.
 - Restriction set - you specify a set of restrictions that must be met before being granted access.
- Activity Completion - you define how you track your completion and expectations for an activity completion date.

3.4.1.3 Files

It allows you to upload files with any extension within the Moodle platform and place them in the course.

To add a file inside a topic, follow these steps:

1. Access to the course editing mode ("notepad") must be enabled on the course website.

2. Under the topic where the file is to be placed, click on "Add activity or resource."
3. In the list of activities, find the file and click on the resource icon.

Basic resource settings:

- Name - the name of the file, visible to course participants.
- Description - files description visible to course participants.
- Select file - sends a file through the activity window or in the form of drag and drop.
- Appearance - you specify how the file should be displayed on the course page, and additionally allows you to display the file size, type, and date of transfer; there are four options to choose from:
 - Automatically.
 - Embedded - the file is embedded within the Moodle platform, leaving the course header and blocks behind.
 - Force download - opens a file, it must be downloaded by the user.
 - Open - the file is opened under the current tab.
 - In a pop-up window - the file is opened in a new browser window.
- Standard module options - you determine the availability (whether the activity should be visible to students), optionally adding an id number and a group mode in the case of many groups.
- Access limitation - you specify the activity availability only for individual users; you can choose from the following options:
 - Cohort - limited to a specific student cohort only.
 - Complete an Activity - requires another activity to be completed before access.
 - Date - you define access only at a specific time.
 - Assessment - the requirement to obtain an appropriate grade (as a percentage) for another activity.
 - Password - requires a password to access the resource.
 - Roles - you define access based on the user's role in the course.
 - Restriction set - you specify a set of restrictions that must be met before being granted access.

- Activity Completion - you define how you track your completion and expectations for an activity completion date

3.4.2 Folders

The folder allows the teacher to add a directory in which he or she can then put files. A folder is useful if you need to transfer a large number of files or need to group them together.

To add a folder to a topic, follow these steps:

1. Access to the course editing mode ("notepad") must be enabled on the course website.
2. Under the topic in which the folder is to be placed, click on "Add activity or resource."
3. In the list of activities, find a folder and then click on the resource icon.

Basic resource settings:

- Name - the name of the file, visible to course participants.
- Description - file description visible to course participants.
- Content - allows you to upload files to the directory:
 - Files - allows you to transfer files to a directory; files can be uploaded independently or in the form of a single .zip file which can later be unpacked.
 - Display folder contents - allows you to set the way of displaying the folder contents. You can choose to display the contents on a new page or the course's main page. Additionally, you can select options such as show directory structure, show download folder button, and force download files.
- Standard module options - you determine the availability (whether the activity should be visible to students), optionally adding an id number and a group mode in the case of many groups.
- Access limitation - you specify the activity availability only for individual users; you can choose from the following options:

- Cohort - limited to a specific student cohort only.
 - Complete an Activity - requires another activity to be completed before access.
 - Date - you define access only at a specific time.
 - Assessment - the requirement to obtain an appropriate grade (as a percentage) for another activity.
 - Password - requires a password to access the resource.
 - Roles - you define access based on the user's role in the course.
 - Restriction set - you specify a set of restrictions that must be met before being granted access.
- Activity Completion - you define how you track your completion and expectations for an activity completion date.

3.4.3 Tasks

The task allows the teacher to collect students' work, evaluate them and comment on them. It is a very useful activity in which students can submit their works in the form of files of any type and a collection of files in a compressed format (e.g., zip, rar). The teacher can leave a comment or upload files as part of the answer.

To add a task inside a topic, follow these steps:

1. On the course website, you must enable access to the course editing mode ("notepad").
2. Under the topic where the task is to be placed, click "Add activity or resource."
3. In the list of activities, find a task and click on the resource icon.

Basic resource settings:

- Name - the name of the folder, visible to course participants.
- Description - description of the folder visible to course participants.
- Additional files - additional files visible to the course participants, e.g. the content of the task in the form of a pdf file.

- Availability - you determine the availability of the task for course participants:
 - Allow task submission ~~from~~ - you define the date from which students can submit their task solutions.
 - Deadline for submission - the deadline by which students must send their solutions to the tasks. If the task allows submission of work after this date, the task will be defined as late.
 - Deadline - the date after which students cannot submit solutions.
 - Remind me to evaluate - this is the date visible to the teacher in the cockpit and calendar, reminding me to check the solutions sent by the course participants.
- Types of tasks
 - Types of tasks - you define the form of submitting tasks; there are two options to choose from:
 - Online text and recording - students can post solutions using the HTML editor.
 - Word limit - defining the maximum number of words the student can send as part of the solution.
 - Uploaded files - students can upload solutions as uploaded files:
 - Maximum number of transferred files - you determine the maximum number of files that can be transferred by the student in the form of a solution.
 - Maximum size of the transferred file - the maximum size that the student can send the solution.
 - Accepted file types - you define what types of files can be sent by the student as part of solving the task.
- Types of feedback - you determine the form of the feedback given to the student by the teacher; four types can be distinguished:
 - Feedback - sends a feedback comment to the task posted by the student.

- PDF Annotation - allows PDF solutions to display them and add notes, drawings, and comments directly on the student's work.
- Off-line evaluation sheet - enables the teacher to download and send a sheet with student grades.
- Comments files - enables the teacher to send files with comments to the students.
- Group task settings - assigns a task to a specific group of students.
- Content - allows you to send files to the directory:
 - Files - sends files to a directory; files can be uploaded independently or in the form of one .zip file, which can later be unpacked.
 - Display folder contents - sets the method of displaying the folder contents; you can choose to display the contents on a new page or the course's main page. Additionally, you can select options such as show directory structure, show download folder button, and force download files.
- Standard module options - you determine the availability (whether the activity should be visible to students), optionally adding an id number and a group mode in the case of many groups.
- Access limitation - you specify the activity availability only for individual users; you can choose from the following options:
 - Cohort - limited to a specific student cohort only.
 - Complete an Activity - requires another activity to be completed before access.
 - Date - you define access only at a specific time.
 - Assessment - the requirement to obtain an appropriate grade (as a percentage) for another activity.
 - Password - requires a password to access the resource.
 - Roles - you define access based on the user's role in the course.
 - Restriction set - you specify a set of restrictions that must be met before being granted access.

3.4.4 Virtual Programming Lab

The Virtual Programming Lab (VPL) enables the teacher to collect programming work in many programming languages and present students' work in real time. This activity makes it possible to create programmes in almost any programming language, save a copy of the created programme and its compilation, debugging, and observing the results obtained.

To add a VPL inside a topic, follow these steps:

1. On the course website, you must enable access to the course editing mode ("notepad").
2. Under the topic in which the task is to be placed, click on "Add activity or resource."
3. In the list of activities, find the Virtual Programming Lab and then click on the resource icon.

Basic activity settings:

- Name - the name of the VPL, visible to course participants.
- Short description - short information about the VPL visible to participants.
- Description - description of the VPL visible to course participants.
- Work submission period - specify the period during which the activity will be available to course participants.
- Available from - you specify the date after which the activity will be available to course participants.
- End date - you specify the date after which the activity will cease to be available to course participants, which results in the impossibility of further editing the submitted works or sending new works.
- Restrictions on submitting works - you define restrictions on submitting works.
- Maximum number of files - the maximum number of files (programmes) that a course participant can upload or create.
- Uploading an external file, paste and drop external content - you specify whether a course participant should be able to upload a ready file with the

programme and also be able to copy content from an external file to a created file inside the VPL.

- Maximum file upload size - you define the maximum length of a course sent by a course participant.
- Password - sets a VPL access password that the course participant must provide to be able to use the activity.
- Standard module options - you determine the availability (whether the activity should be visible to students), optionally adding an id number and a group mode in the case of many groups.
- Access limitation - you specify the activity availability only for individual users; you can choose from the following options:
 - o Cohort - limited to a specific student cohort only.
 - o Complete an Activity - requires another activity to be completed before access.
 - o Date - you define access only at a specific time.
 - o Assessment - the requirement to obtain an appropriate grade (as a percentage) for another activity.
 - o Password - requires a password to access the resource.
 - o Roles - you define access based on the user's role in the course.
 - o Restriction set - you specify a set of restrictions that must be met before being granted access.

3.4.4.1 Compiler Settings

Another important element is setting up the compiler and making it possible to compile, debug and run the programme. To do this, after creating a VPL activity, follow these steps:

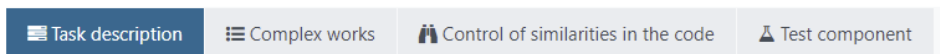
1. On the course page, in the selected topic, click on the name of the added VPL.
2. On the right side, select the option to edit the activity (gear).
3. Choose "Execution options."

Within the execution option, you can set the following option:


- Run script - you specify the compiler of the selected programming language; if you choose the automatic detection option, the compiler compatible with the extension of the transferred file will be chosen.
- Debug script - you specify the debugging language; if you select the automatic detection option, the compiler compatible with the extension of the transferred file will be chosen.
- Run - you define whether the course participant should be able to run his or her programme inside the VPL.
- Debug - you specify if the participant should be able to debug his or her programme inside the VPL.
- Automatic evaluation - specify whether the programme should be automatically checked based on test data.

3.4.4.2 Basic Information About a VPL Activity Created

After clicking on the name of the created activity on the course page, you will see a page with four tabs: Task description, Submitted papers, Code similarity check, and Test component.



Preparation for the colloquium

 **End date:** Wednesday, March 3, 2021,
01:00

Maximum number of

files: 5 **Type of work:** Individual work **Rating settings:** Maximum rating: 100

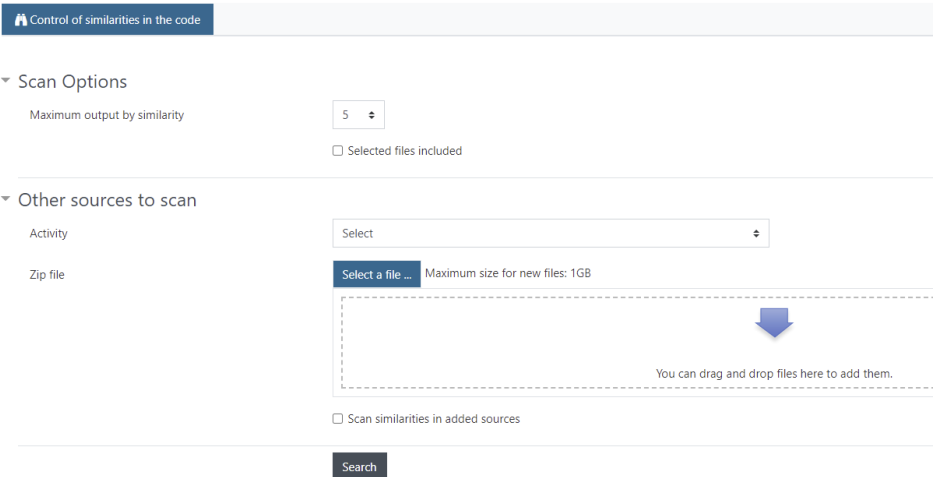
Run: Yes. **Debug:** Yes. **Ratings:** No    

Task description - this is the first tab devoted to the description of the task; in it, you can find a detailed description of the activity, the date of the end of the activity, the maximum number of files to be sent set by the teacher, information about whether the work is performed individually or in groups, the issue of setting grades.

In addition, information is included on whether the submitted code is subject to evaluation by the lecturer and whether the code written by the student can be debugged and run in VPL by the student.

Submitted works - under the 'Composed Works' tab, the teacher has access to all submitted works sent by course participants. The student's name and surname, information about the date of sending the document, the last version of the programme, the number of saved programmes (earlier copies of the code), and a gear wheel are displayed. After clicking on the gear wheel icon, you gain access to additional options, such as a preview of the submitted work, a list of submitted components, options, and the possibility of making a copy.

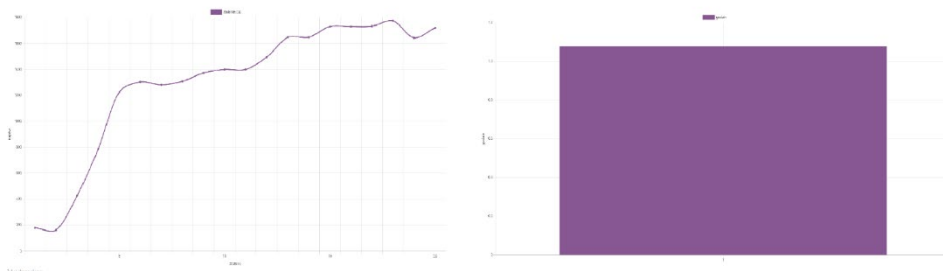
Checking the similarities in the code allows for analysing the similarities between the programmes sent by the course participants. It allows you to check the similarity to other submitted programmes, as well as to the solution sent by the teacher.



Test components - allows you to manage test components

3.4.4.3 Preview of the Submitted Work

As part of the submitted works, you can see a list of submitted components , an incremental graph of the size of the submitted files, and a graph of working time and activity within the task.



#	Date added	Task description	Action
17	tuesday, february 23, 2021, 5:03 pm	Test.cpp 5280b 189l	⚙️ ▾
16	tuesday, february 23, 2021, 5:02 pm	Test.cpp 5286b 189l	⚙️ ▾
15	tuesday, february 23, 2021, 5:01 pm	Test.cpp 5275b 189l	⚙️ ▾
14	tuesday, february 23, 2021, 5:00 pm	Test.cpp 5258b 189l	⚙️ ▾
13	tuesday, february 23, 2021, 4:12 pm	Test.cpp 5251b 189l	⚙️ ▾

After selecting any programme instance, the entire submitted programme is visible.

cos.cpp

```
1 #include <iostream>
2 #include <cstdlib>
3
4 using namespace std;
5
6 int main(){
7     int a;
8     int b;
9     cin >> a;
10    cin >> b;
11    int c = a+b;
12    cout << c << endl;
13 }
```

Additionally, an edit option can be chosen that makes changes in the code, runs it, debugs it, and performs tests at the evaluation level by the test examples created.

A screenshot of a code editor window titled 'cos.cpp'. The editor has a dark background and shows the following C++ code:

```
1
2 #include <iostream>
3 #include <cstdlib>
4
5 using namespace std;
6
7 int main(){
8     int a;
9     int b;
10    cin >> a;
11    cin >> b;
12    int c = a+b;
13    cout << c << endl;
14 }
```

3.4.4.4 Preparation of Test Files and Check Programme

As part of the programme implementation, you can prepare test files to analyse the solution. You can create a test file by selecting the task settings (gear) and selecting test cases.

When creating a test case, its name should be given after the keyword "case", e.g., case = one

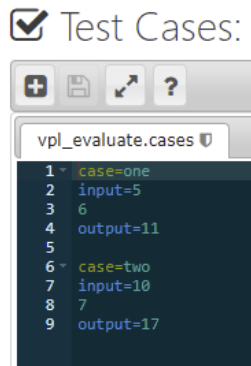
Then provide the input data that will be assigned to the values entered from the keyboard, e.g. (the two numbers to be added are entered, separated by an "enter" key - number 5 and number 6)

Input = 5

The next task is to pass the result of the operation after the keyword "output", e.g.

Output = 11

Sample test file (Test Cases):



3.4.5 Jupyter Notebook

Jupyter Notebook is an open-source web application. It allows the creation and sharing of documents with live code, various equations, visualisations, etc. Among the users of Jupyter Notebook, we can distinguish between numerical simulations, statistical modelling, machine learning, etc.

It is most often used as an application to create programmes in Python language and then analyze them. As part of Moodle, an instance of a virtual machine is created for each student, on which the student can create files. When creating a programme, the teacher does not have access to the created programme, so a good solution is to allow the student to upload the finished programme using a different activity.

After the end of the lesson, the programme is still available to the student for the time established by the administrators of the Moodle platform. The time of availability is defined as the time since the last launch of the programme by the student.

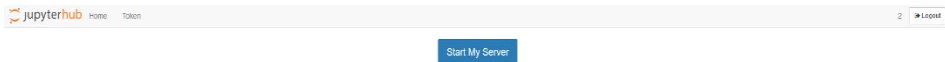
As part of the course, the teacher can add the Jupyter Notebook activity in the following way:

1. On the course website, you must enable access to the course editing mode ("notepad").
2. Under the topic in which the task is to be placed, click on "Add activity or resource."

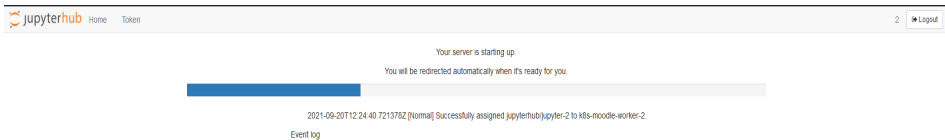
3. In the list of activities, find the Jupyter Notebook and then click on the resource icon.



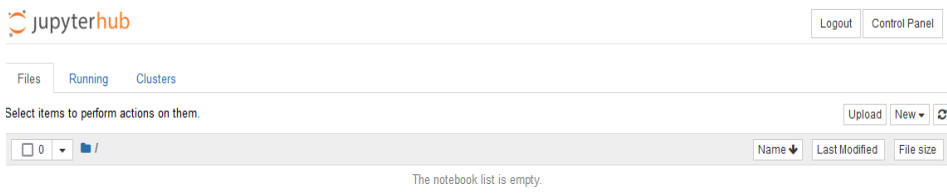
After clicking on the activity, the student can start his Notebook.



Then a virtual machine is created for the student to operate the Jupyter Notebook.



Once created, the student has the option to create their programme.



4 Assessing Students

This section describes the basic type of quiz designed for the examination and assessment of students.

4.1 Quiz

In this subsection, we present the basic test quiz.

4.1.1 Test Quiz

The Quiz test is an online real-time test in which the student has the opportunity to answer questions at the time specified by the teacher, which can then be checked automatically or manually by the teacher (depending on the type of questions described in the section questions types).

To create a Test Quiz activity, follow these steps:

1. Access to the course editing mode ("notepad") must be enabled on the course website.
2. As part of the topic in which the test quiz is to be placed, click on "Add activity or resource."
3. In the list of activities, find the test quiz and click on the activity icon.

Basic resource settings:

- Name - the name of the folder, visible to course participants.
- Description - description of the folder visible to course participants.
- Time - you define the date (day, hour) when the test will be available and its duration:
 - Open the test - the date on which the test becomes available to students (it is possible to start the test); if it is not enabled, the test is available continuously.
 - Close the test - you specify the date (day, time) on which the test is no longer available to students. They cannot start the test. If it is not enabled, the test is available continuously after opening.
 - Time limit - the time during which the student can write the test, starting from the moment the student starts the test.
 - After the time expires – it allows the supervisor to decide how the test should behave after the end of the test; you can choose one of three options:
 - Open approaches are saved automatically - after completing the test (timeout), the student's open approach

- is closed, and the answers given so far are saved and transferred for evaluation.
- Existing grace period - you specify the time that begins after exceeding the time limit and allows the student to review and approve their answers. Still, the student cannot answer new questions.
 - Attempts must be approved before the end of time - when selected, approaches that are not completed by the student and approved before the end of time are not validated.
 - Assessment - you define the method of assessment.
 - Assessment category - if you create a grade category, you can assign to which category the grade for the quiz should be assigned.
 - Passing threshold - you define the threshold at which the test is passed; it is used, among other functions, in the grading log, where quizzes taken are marked in green and failed quizzes in red.
 - Available approaches - you define how many times the student is allowed to take the quiz.
 - Assessment method - if you select that the student can take the quiz more than once, it allows you to specify how the quiz grade should be determined; there are several options to choose from:
 - Top grade.
 - Average grade.
 - The first attempt.
 - The last attempt.
 - Layout - you define basic information about the layout of the test view and how to view it:
 - Number of questions per page - divides the test into pages, and you determine how many questions should be visible on a single page; this is useful for long tests.
 - Navigation method - you define the way the student can view the quiz; there are two options to choose from:
 - Any - the student can freely navigate through the test, and move to the next and previous questions.

- Sequential - after answering the question, the student cannot return to it to change the answer.
- Questions Behavior - you specify how questions should be displayed and how questions should behave after answering:
 - Change the order inside the question - in the case of multiple-choice questions, it allows you to change the order of answers for each student taking the quiz.
 - How the questions behave - you define the behaviour of questions after the student answers or during the answer; there are several options to choose from:
 - Feedback after completion of the CBM approach.
 - Interactive with repetitions - if this option is selected, student see that they made a mistake immediately after answering and then has the option of correcting it, which, however, results in receiving a smaller number of points for the answer.
 - Immediate feedback - the student immediately after answering can see if the answer was correct.
 - Instant feedback from CBM.
 - Manual grading.
 - Delayed feedback - students answer questions, and only after all answers have been approved, they receive a grade and comment.
 - Adaptive mode.
 - Adaptive mode (no penalty).
- Review options - change the view for the student during and after the quiz, depending largely on the chosen behaviour of the questions and the inclusion of the duration.
 - You can specify the following options:
 - While testing (only available for interactive and immediate feedback modes) – it can be viewed while writing the test.
 - Immediately after the test - it can be viewed immediately after the end of the test (approx. 2 minutes).

- Later, while the test is still open - it can be viewed as long as the test is open.
- After closing the test - when the time has elapsed during which the test is available for all students to solve.
- The following items can be specified for each option:
 - Rehearsal - you specify whether the student can see his or her approach to the quiz.
 - Is correct – you display information to the student about the answer given by him or her as 'Correct', 'Partially correct' or 'Incorrect'.
 - Points - information about the number of points obtained for a specific task and the total number of points obtained for the entire quiz.
 - Detailed feedback - information prepared by the lecturer, which is displayed after the student has answered.
- Standard module options - you determine the availability (whether the activity should be visible to students), optionally adding an id number and a group mode in the case of many groups.
- Access limitation - you specify the activity availability only for individual users; you can choose from the following options:
 - Cohort - limited to a specific student cohort only.
 - Complete an Activity - requires another activity to be completed before access.
 - Date - you define access only at a specific time.
 - Assessment - the requirement to obtain an appropriate grade (as a percentage) for another activity.
 - Password - requires a password to access the resource.
 - Roles - you define access based on the user's role in the course.
 - Restriction set - you specify a set of restrictions that must be met before being granted access.

After creating a quiz, it is possible to fill it in with previously prepared questions or to create new questions.

To add questions to the quiz, follow these steps:

1. On the course page, find the quiz activity you added.
2. Enter the chosen quiz by clicking on its name.
3. On the right side of the quiz window, find a gear icon and click on it (it is not the same gear as for the course management).
4. Select the option "Edit test content" from the drop-down list.

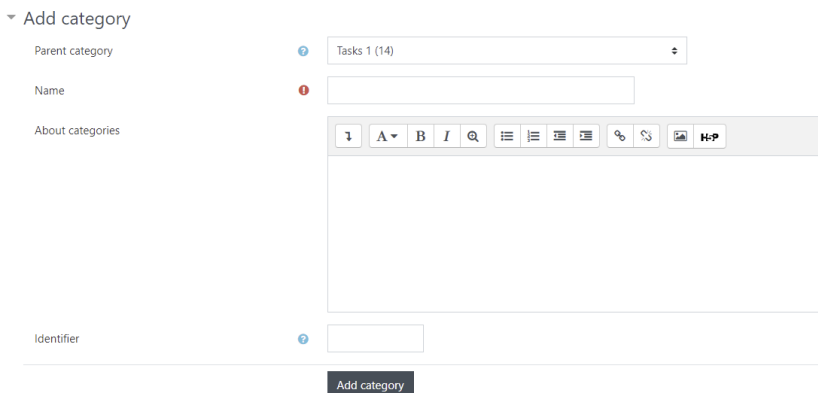
4.2 Question Database

4.2.1 Categories

This section describes the basics of creating categories and adding questions to categories. Categories are treated as directories into which questions can then be placed. They also allow you to create a hierarchical structure. The use of categories is considered good practice and allows you to break down the questions you create into some linked structures of a similar nature, which is great for creating random question quizzes.

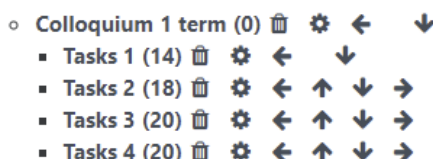
To create a category, follow these steps:

1. Enable access to course management ("gears").
2. On the Question Bank page, select the Question Category.
3. At the bottom of the page, there is a button for adding a new category.



The screenshot shows the 'Add category' form in Moodle. It includes a dropdown menu for 'Parent category' (set to 'Tasks 1 (14)'), a text input field for 'Name', a rich text editor for 'About categories', and a text input field for 'Identifier'. A blue 'Add category' button is located at the bottom of the form.

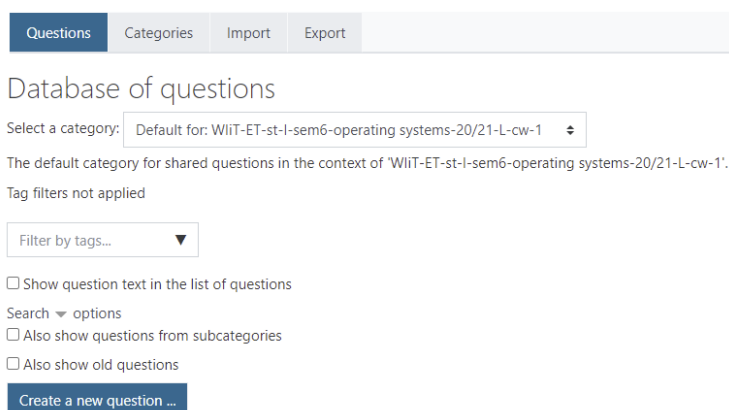
The most important element is to define the parent category in which the new category will be placed, then the name of the category and optional information about the category should be provided. Once created, it can also be moved elsewhere, modified, or deleted.



4.3 Question Types

This section describes the basic question types that can be created within the course and the general way to add questions. To add a new question, follow these steps:

1. Enable access to course management ("gears")
2. In the Question bank panel, select Question database
3. Specify the category to which the question should be added



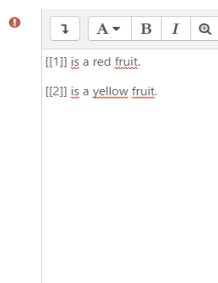
4.3.1 Drag and Drop

Question type where missing words in the text are filled with labels by drag and drop. When creating a question, the number of the label you want to place in the right place is specified in double square brackets.

Basic question settings:

- Current category - the current category in which the option to add a question has been selected, the question will be added to it.
- Save in category - in case of resignation from the current category, you can select the category in which the question should be located from the drop-down menu.
- Question name - the name displayed on the list of questions, helping to identify the question (but it is not visible to students).
- Content of the question - the content of the question intended for students:

Content of the question



- Default score - the default number of points to be obtained for the question (may be scaled when creating a test for students).
- General feedback - information is displayed to students after answering a question.
- ID - optional ID of the question must be unique.
- Choices - define the labels that can be added:
 - Random - selecting this option changes the order in which the labels are displayed randomly.
 - Choice [[n]] - where "n" is a number, which is the identifier to be entered in the text of the question as to the correct answer (to increase the pedagogic level of difficulty for students, you can add more labels than there are correct answers).
 - Answer - the content of the label.
 - Group - you define the label group (they differ in colours when displaying the question), e.g.

▼ Election

Randomly

Selection [[1]] Answer Group Infinity

Selection [[2]] Answer Group Infinity

Selection [[3]] Answer Group Infinity

Selection [[4]] Answer Group Infinity

- Complex feedback - you add additional information for the student to be displayed after answering:
 - For each correct answer - information is displayed if a correct answer is given.
 - For each partially correct answer – information is displayed when a partially correct answer is given.
- Multi-trial settings - necessary settings if the student is allowed to approach a question multiple times:
 - Penalty for each incorrect answer - reduction is expressed as a percentage of the possible points in the case of an incorrect answer.
 - Tip - advice aimed at helping the student.
 - Hint options - you clear only incorrect answers and display the number of correct answers to the student.
- Save changes - after pressing the save changes button, the question is added to the selected category.

View of an example question created based on the above description:

is a red fruit.

is a yellow fruit.

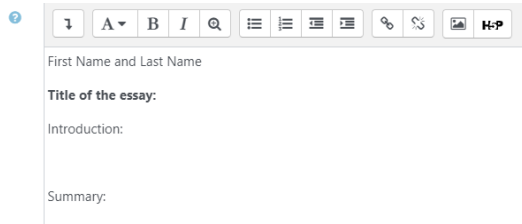
4.3.2 Essay

Question type that allows the student to answer by sending a file or filling in the editor field. Essay-type tasks must be manually graded by the tutor.

Basic question settings:

- Category - you select the category in which the question should be placed from the drop-down menu.
- Name of the question - the name is visible on the list of questions to help identify the question (but it is not visible to students).
- Content of the question - the content of the task is visible to students.
- Default score - the default number of points to be obtained for the question (it can be scaled when creating a test for students).
- General feedback - information is displayed to students after answering a question.
- ID - optional ID of the question must be unique.
- Response options - basic response options, we can distinguish:
 - Response format - you define the format of the response field for the student:
 - HTML editor - the editor field allows you to type using an HTML editor, insert links, images, equation editor, etc.
 - HTML editor with file selection - additionally allows you to insert audio/video recordings, word templates, etc.
 - Plain Text - Only keyboard text can be entered.
 - Required text - you specify whether the text field must contain content for the question to be sent.
 - Input field size - you define the number of lines of text visible to the student.
 - Allow attachments - allows students to upload files with solutions.
- Response template - you enter a template that is visible to the student and allows you to standardise the answers or indicate the form of the answer.

Response template



The screenshot shows a Moodle response template editor. At the top, there is a toolbar with various icons for text formatting (bold, italic, underline, link), list creation, and other editing tools. Below the toolbar, the text area contains the following content:

First Name and Last Name

Title of the essay:

Introduction:

Summary:

- Save changes - after pressing the save changes button, the question is added to the selected category.

The screenshot shows a question editor interface. On the left, a summary box displays: "Question 1", "No response", and "Points: 1,00". The main editor area is titled "Write an essay" and contains a rich text toolbar with icons for undo, font color, bold, italic, link, bulleted list, numbered list, table, link, unlink, redo, and image. Below the toolbar, the form includes a "First Name and Last Name" field, a "Title of the essay:" label, an "Introduction:" label, and a "Summary:" label.

4.3.3 Matching

Question type in which the content area and the list of names (possible to choose, displayed in the form of a drop-down menu) must be appropriately matched to the content.

Basic question settings:

- Category - you select the category in which the question should be placed from the drop-down menu.
- Name of the question - the name is visible on the list of questions, helping to identify the question (but it is not visible to students).
- Content of the question - the content of the task is visible to students.
- Default score - the default number of points to be obtained for the question (it can be scaled when creating a test for students).
- General feedback - information is displayed to students after answering a question.
- ID - optional ID of the question must be unique.
- Answers - you enter questions and answers. It is necessary to provide at least two questions (content area) and three answers (name list). To add additional incorrect answers, leave the question field blank.

▼ Response

Available options

You must provide at least two questions (left column) and three answers (right column). You can provide additional items where both question and answer are empty will be ignored.

Question 1	<p>England (England)</p>
Answer	<p>London</p>
Question 2	<p>Italy</p>
Answer	<p>Rome</p>
Question 3	
Answer	<p>Paris</p>

- Complex feedback - you add additional information for the student to be displayed after answering:
 - For each correct answer - information is displayed if a correct answer is given.
 - For each partially correct answer - information is displayed when a partially correct answer is given.
- Multi-trial settings - necessary settings to allow the student to approach a question repeatedly:
 - Penalty for each incorrect answer - reduction is expressed as a percentage of possible points in the case of an incorrect answer.
 - Tip - advice aimed at helping the student.
 - Hint options - you clear only incorrect answers and display the number of correct answers to the student.
- Save changes - after pressing the save changes button, the question is added to the selected category

Question 1 No response Points: 1.00	Match the capital city to the country. England (England) <input type="text" value="Select..."/> Italy <input type="text" value="Select..."/>
<input type="button" value="Start again"/> <input type="button" value="Save"/> <input type="button" value="Fill in with correct answers"/> <input type="button" value="Approve and finish"/> <input type="button" value="Close preview"/>	<input type="text" value="Select..."/> <input type="text" value="Paris"/> <input type="text" value="London"/> <input type="text" value="Rome"/>

4.3.4 Matching by Drag and Drop

The question type in which the content area appears and the list of names (you can see them on the right side of the question) that must be appropriately matched to the content.

Basic question settings:

- Category - you select the category in which the question should be placed from the drop-down menu.
- Name of the question - the name is visible on the list of questions; it helps identify the question (but it is not visible to students).
- Content of the question - the content of the task is visible to students.
- Default score - the default number of points to be obtained for the question (it can be scaled when creating a test for students).
- General feedback - information is displayed to students after answering a question.
- ID - optional ID of the question must be unique.
- Answers - you enter questions and answers. It is necessary to provide at least two questions (content area) and three answers (name list). To add additional incorrect answers, leave the question field blank.
- Complex feedback - you add additional information for the student to be displayed after answering:
 - For each correct answer - information is displayed if a correct answer is given.
 - For each partially correct answer - information is displayed when a partially correct answer is given.
- Multi-trial settings - necessary settings to allow the student to approach a question repeatedly:
 - Penalty for each incorrect answer - reduction is expressed as a percentage of possible points in the case of an incorrect answer.
 - Tip - advice aimed at helping the student.
 - Hint options - you clear only incorrect answers and display the number of correct answers to the student.

- Save changes - after pressing the save changes button, the question is added to the selected category



The screenshot shows a Moodle question interface. On the left, a box contains the question details: "Question 1", "No response", and "Points: 1.00". The main content area displays the question text: "Match the capital city to the country." Below this, there are two categories listed: "Italy" and "England (England)". To the right of the categories, there are two empty input boxes, each with the placeholder text "Drag the answer here". On the far right, there is a list of possible answers: "Paris", "London", and "Rome", each in its own input box.

4.3.5 Multiple Choice

Question type that allows you to create a selection task with one or more correct answers.

Basic question settings:

- Category - you select the category in which the question should be placed from the drop-down menu.
- Name of the question - the name is visible on the list of questions, helping to identify the question (but it is not visible to students).
- Content of the question - the content of the task is visible to students.
- Default score - the default number of points to be obtained for the question (it can be scaled when creating a test for students)
- General feedback - information is displayed to students after answering a question.
- ID - optional ID of the question must be unique.
- Shuffle answers - selecting this option causes the random selection of answers on the list of answers.
- One or more answers? - select from the drop-down menu whether the question contains one correct answer or many correct answers.
- Numbering of responses - you choose the method of numbering the answers.
- Show standard instructions - you choose whether an instruction for answering should appear before the question, e.g., "select one answer", or "select all correct answers".

- Responses - you enter the answers and score them accordingly:
 - When selecting: Only one answer:
 - One of the answers should be given 100%.
 - If the other answers are chosen to mark none, 0 points are given for the incorrect answer.
 - If you choose negative values for the remaining answers if you choose a wrong answer, negative points are given by the percentage.
 - When selecting: More than one answer:
 - The sum of points for correct answers must be 100%.
 - If the remaining answers are chosen, no points are deducted, and no points are deducted for incorrect answers, so the student, by selecting all answers, gets 100% of the points.
 - If you choose negative points for the remaining answers, they are subtracted from the maximum number of points; choosing - 100% resets the result when selecting the correct and incorrect answer.
 - It is impossible to set receiving points only if you select all correct answers; for this, you can use the task: All or nothing.
- Complex feedback - you add additional information for the student to be displayed after answering:
 - For each correct answer - information is displayed if a correct answer is given.
 - For each partially correct answer - information is displayed when a partially correct answer is given.
- Multi-trial settings - necessary settings if the student is allowed to approach a question multiple times:
 - Penalty for each incorrect answer - reduction is expressed as a percentage of the possible points in the case of an incorrect answer.
 - Tip - advice aimed at helping the student.
 - Hint options - you clear only incorrect answers and display the number of correct answers from the students.

- Save changes - after pressing the save changes button, the question is added to the selected category.

Response

Choice 1	<input type="button" value="↓"/> <input type="button" value="A"/> <input type="button" value="B"/> <input type="button" value="I"/> <input type="button" value="Q"/>
	4
Assessment	100% <input type="button" value="↓"/>
Feedback	<input type="button" value="↓"/> <input type="button" value="A"/> <input type="button" value="B"/> <input type="button" value="I"/> <input type="button" value="Q"/>

Choice 2	<input type="button" value="↓"/> <input type="button" value="A"/> <input type="button" value="B"/> <input type="button" value="I"/> <input type="button" value="Q"/>
	6
Assessment	No <input type="button" value="↓"/>
Feedback	<input type="button" value="↓"/> <input type="button" value="A"/> <input type="button" value="B"/> <input type="button" value="I"/> <input type="button" value="Q"/>

Choice 3	<input type="button" value="↓"/> <input type="button" value="A"/> <input type="button" value="B"/> <input type="button" value="I"/> <input type="button" value="Q"/>
	8
Assessment	-100% <input type="button" value="↓"/>
Feedback	<input type="button" value="↓"/> <input type="button" value="A"/> <input type="button" value="B"/> <input type="button" value="I"/> <input type="button" value="Q"/>

4.3.6 All or Nothing Multiple Choice

A question type that creates a selection task with one or more correct answers, giving 100% if you selected all correct answers or 0% if you selected any incorrect answers or did not select all correct answers.

Basic question settings:

- Category - you select the category in which the question should be placed from the drop-down menu.
- Name of the question - the name is visible on the list of questions, helping to identify the question (but it is not visible to students).
- Content of the question - the content of the task is visible to students.
- Default score - the default number of points to be obtained for the question (it can be scaled when creating a test for students).

- General feedback - information is displayed to students after answering a question.
- ID - optional ID of the question; it must be unique.
- Shuffle answers - selecting this option causes the random selection of answers on the list of answers.
- One or more answers - you select from the drop-down menu whether the question contains one correct answer or many correct answers.
- Numbering of responses - you choose the method of numbering the answers, e.g. A, B, C or 1, 2, 3, etc.
- Responses – you enter answers and information on whether the answer is correct or not. To receive points, the student must select all answers marked as correct.
- Complex feedback - you add additional information for the student to be displayed after answering:
 - For each correct answer - information is displayed if a correct answer is given.
 - For each partially correct answer - information is displayed when a partially correct answer is given.
- Multi-trial settings - necessary settings if the student is allowed to approach a question multiple times
 - Penalty for each incorrect answer - reduction is expressed as a percentage of the possible points in the case of an incorrect answer.
 - Tip - advice aimed at helping the student.
 - Hint options - you clear only incorrect answers and display the number of correct answers from the students.
- Save changes - after pressing the save changes button, the question is added to the selected category.

4.3.7 Short answer

A question type that allows the student to enter a short answer of several words, which is then compared to the entered patterns.

Basic question settings:

- Category - you select the category in which the question should be placed from the drop-down menu.
- Name of the question - the name is visible on the list of questions, helping to identify the question (but it is not visible to students).
- Content of the question - the content of the task is visible to students.
- Default score - the default number of points to be obtained for the question (it can be scaled when creating a test for students).
- General feedback - information is displayed to students after answering a question.
- ID - optional ID of the question, must be unique.
- Case-sensitive – you define whether the student's entered letters are case sensitive.
- Answers - you enter the answers (answer patterns) and the appropriate number of points due to them. The symbol "*" stands for any character
- Complex feedback - you add additional information for the student to be displayed after answering
 - For each correct answer - information is displayed if a correct answer is given.
 - For each partially correct answer - information is displayed when a partially correct answer is given.
- Multi-trial settings - necessary settings if the student is allowed to approach a question multiple times:
 - Penalty for each incorrect answer - reduction is expressed as a percentage of the possible points in the case of an incorrect answer.
 - Tip - advice aimed at helping the student.
 - Hint options - you clear only incorrect answers and display the number of correct answers from the students.
- Save changes - after pressing the save changes button, the question is added to the selected category.

4.3.8 Numerical

Question type that allows you to enter a numerical answer that is checked by comparing it with the pattern introduced by the teacher, taking into account the tolerance (e.g. rounding off).

Basic question settings:

- Category - you select the category in which the question should be placed from the drop-down menu.
- Name of the question - the name is visible on the list of questions, helping to identify the question (but it is not visible to students).
- Content of the question - the content of the task is visible to students.
- Default score - the default number of points to be obtained for the question (it can be scaled when creating a test for students).
- General feedback - information is displayed to students after answering a question.
- ID - optional ID of the question, must be unique.
- Case-sensitive - you define whether the student's entered letters are case sensitive.
- Responses - you enter answers in numerical form, including an acceptable error and a grade for a given answer.
- Unit related settings - you enter units as an element of evaluation:
 - Unit related settings - three options can be selected, units are not used, the unit is optional or necessary.
 - Decreasing the grade for error in the unit - in the case of selecting the option that the unit is necessary, it is possible to designate in the range (0-1) for how many percent of points are subtracted for the wrong unit.
 - Unit entered via - you define how the unit should be entered. There are three options to choose from, a text box, a button, and a drop-down list.
 - The unit stands up - you specify whether a unit should appear before or after a numerical value.

- Units - you enter the correct unit.
- Multi-trial settings - necessary settings if the student is can answer a question multiple times.
 - Penalty for each incorrect answer - reduction is expressed as a percentage of the possible points in the case of an incorrect answer.
 - Tip - advice aimed at helping the student.
 - Hint options - you clear only incorrect answers and display the number of correct answers from the students.
- Save changes - after pressing the save changes button, the question is added to the selected category.

4.3.9 True/False

True / False question type.

Basic question settings:

- Category - you select the category in which the question should be placed from the drop-down menu.
- Name of the question - the name is visible on the list of questions, helping to identify the question (but it is not visible to students).
- Content of the question - the content of the task is visible to students.
- Default score - the default number of points to be obtained for the question (it can be scaled when creating a test for students).
- General feedback - information is displayed to students after answering a question.
- ID - optional ID of the question, must be unique.
- Correct answer – you determine whether the correct answer is marked true or false by the student.
- Multi-trial settings - necessary settings if the student is allowed to approach a question multiple times:
 - Penalty for each incorrect answer - reduction is expressed as a percentage of the possible points in the case of an incorrect answer.
 - Tip - advice aimed at helping the student.

- Hint options - you clear only incorrect answers and display the number of correct answers from the students.
- Save changes - after pressing the save changes button, the question is added to the selected category.

4.4 Import Questions

This section describes how to import course questions from a previously created file.

To import questions to the course, follow these steps:

1. Enable access to course management ("gears")
2. In the Question bank pane, select Import
3. Select the format of the question file you want to import
4. Select the main category to which the questions should be imported
5. Determine what the system should do when an error occurs
6. Placing the question file via the activity window or drag and drop the file
7. Click on the import button

4.5 Export Questions

This section describes how to export questions from a course to a file that you can use to import in another course in the future. In Moodle, you can export questions to several basic formats, detailed in Formats and Examples of files with questions. In the case of questions with an attached multimedia file, it is recommended to use the Moodle XML file.

To export course questions to a file, follow these steps:

1. Enable access to course management ("gears")
2. In the Question bank panel, select Export
3. Select the format of the question file to which you want to export
4. Select the main category from which the export is to be performed (subcategories of the selected category are automatically included)
5. Click on the Export questions to file button

5 Backup and Restore

This chapter describes how to backup a created course and how to restore a course from a created template with data.

5.1 Backup

This section describes how to back up your course. The teacher within his or her course has the option to back up selected parts of the course, which can be used to maintain the history of the course being conducted or to create a new course using the topics and data included in the current course. This copy can be generated and saved to disk in an offline form.

To create a backup file of your course, follow these steps:

1. Enable access to course management ("gears")
2. In the Course Settings pane, select Backup
3. Select Backup settings, which allow you to define what the backup should contain. The most important elements include: including course users, activities, resources, blocks, files, question bank, and groups
4. Select the scheme settings and include the individual activities within the copy
5. At the bottom of the page, click on the backup button

5.2 Course Restoring

This section describes how to restore your course from a backup. The previously created backup file in the .mbz format allows you to restore the course together with the data contained in the backup.

To restore a course from a backup, follow these steps:

1. Enable access to course management ("gears")
2. In the Course Settings pane, select Restore
3. Select the file to import through the activity field or by drag and drop
4. At the bottom of the page, click on Restore

Conclusions

The developed document is based on an analysis of websites and the authors' own experience. The main document that contributed to the development of the handbook was the Moodle documentation available at [www:https://docs.moodle.org](https://docs.moodle.org). The Moodle documentation provides fully detailed descriptions of all components, but due to its universal nature does not correspond 100% to the template used in the project.

In the future, the authors of the user guide will introduce additional information on the new features implemented in Moodle and added to the platform used and, in the event of receiving feedback from users, will supplement the existing version with elements that may help to better understand and use the platform. The authors also plan to develop short instructional videos to further facilitate the management of the platform for both the administrator and the teachers.

References

- Moodle Documentation [online], <https://docs.moodle.org>
Instrukcje Politechniki Poznańskiej [online], <https://instrukcje.put.poznan.pl>
Centrum kształcenia na odległość Uniwersytet Śląski w Katowicach [online],
<http://cko.us.edu.pl/cko/faqstudent/102-lista-pomocy-dla-wykladowcy.html>
Instrukcje Uniwersytet Warszawski [online],
https://portal.uw.edu.pl/documents/5755113/6159244/Nowy_moodle_dla_prowadzacych.pdf
University of Massachusetts Amherst [online], <https://www.umass.edu/it/support/moodle>



CYBER SECURITY - TRAINING STUDENTS AND SCHOLARS FOR THE CHALLENGES OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN RESEARCH AND STUDIES FOR INTERNATIONALISATION: HANDBOOK

TATJANA WELZER DRUŽOVEC (ED.)

University of Maribor, Maribor, Slovenia
tatjana.welzer@um.si

Abstract This handbook is a product of the Erasmus+ Strategic Partnership between the partners Université Polytechnique Hauts-de-France, Politechnika Poznanska, Brandenburgische Technische Universität Cottbus-Senftenberg and the coordinator University of Maribor. Contentuous contribution were made by staff of University of Maribor and Politechnika Poznanska, evaluations by staff of the other two partners. The handbooks handles virtual learning environments in the international education and research area and exposure of the systems to cybercrime. Besides introductory contributions on legal aspects of challenges in the fields of human rights, European regulations of data security, civil law and criminal law aspects of cayer security of virtual learning environments and methodologies of their introduction within organisations. The handbook also gives useful instructions for elaboration of virtual courses within virtual learning environments relevant for the internationalised research and education not only since the COVID-19 pandemic. The handbook is dedicated to use on the internet within the Moodle system.

Keywords:

cyber security,
virtual learning
environment,
data security,
cyber crime,
systems

b.tu

Brandenburgische
Technische Universität
Cottbus - Senftenberg

 **Université
Polytechnique**
HAUTS-DE-FRANCE



ATHENA



Sofinancira program
Evropske unije
Erasmus+

