COURSE DESCRIPTION CARD - SYLLABUS

Course name
Data protection [S2IBiJ1-JiEwBP>OD]

Course

Field of study
Safety and Quality Engineering

Year/Semester
2/3

Area of study (specialization)
Quality and Ergonomics in Work Safety

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
15

Laboratory classes
0

Other
0

Tutorials
15

Projects/seminars
0

Number of credit points

2,00

Coordinators

dr inż. Marek Goliński
marek.golinski@put.poznan.pl

Lecturers

Prerequisites

The student has basic knowledge necessary to understand the social and legal conditions of engineering activities. The student has the ability to use the indicated sources and interpret social phenomena. The student understands the need to expand their competences within the framework of social sciences.

Course objective

Providing students with knowledge of the requirements for entrepreneurs and other organizations in the field of collecting and processing personal data and the principle of legal liability resulting from this.

Course-related learning outcomes

Knowledge:
1. The student knows in-depth development trends and good practices regarding security management, in particular data security in organizations in local and global terms [K2_W04].
2. The student knows in depth the principles of information flow, communication, legal and regulatory conditions affecting data protection, characteristic of the area of organization security management [K2_W14].

Skills:
1. The student is able to use methods and tools for solving complex and unusual problems as well as advanced information and communication techniques characteristic of the professional environment related to data management and protection in organizations [K2_U02].
2. The student is able to select and apply computer-aided tools for solving problems characteristic of managing the sphere of data protection in organizations [K2_U08].

Social competences:
1. The student is critical of his knowledge, is ready to consult experts when solving cognitive and practical problems, continuous training in the IT industry and legal regulations, in particular related to data protection in the area of security management in organizations [K2_K01].
2. A student correctly identifies and resolves dilemmas related to broadly understood security, especially in the area of data, understands the need to make the public aware of the need to shape security in various areas of the organization's functioning [K2_K02].

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture: assessment forming discussions summarizing individual lectures, legal problems solved during classes, giving the opportunity to assess the student's understanding of the issues.
The knowledge acquired during the lecture is verified by two 15-minute colloquia, each of which consists of 5-10 questions, scored differently, the need to pass both colloquia.
Exercises: the knowledge acquired during the exercises is verified by two 15-minute colloquiums, each of which consists of 5-10 questions, scored differently. Both tests must be passed.
Rating scale:
0-50 pkt - 2.0;
51-60 pkt - 3.0;
61-70 pkt - 3.5;
71-80 pkt - 4.0;
81-90 pkt - 4.5;
91-100 pkt- 5.0

Programme content

Lecture:
The concept, genesis and sources of personal data protection law. Definition of personal data, their types and special categories. Rules for the processing of "sensitive" and "ordinary" personal data. Entrusting data processing and data sharing. Rights of persons whose data is processed. Obligations of the controller and data processor. Designation, status and tasks of the data protection officer. Compliance and documentation of personal data protection. Risk assessment.
Exercises:
Case study - personal data processing processes in the company. Types of documents related to selected data processing processes in the company. Contract for a specific task/commission, contract for entrusting the processing of personal data, consent to the use of image, processing of ordinary and sensitive data. Protection of personal data in the workplace. Protection and security of personal data from the point of view of a natural person and a legal person, taking into account the challenges arising from functioning in the digital world.

Course topics

Lecture
Concept, Origins, and Sources of Data Protection Law
Data protection law is a set of regulations governing how personal data is collected, processed, stored, and shared. The origins of this law date back to the 1970s, when the development of information technology began to pose a threat to individual privacy. Key sources of data protection law include the General Data Protection Regulation (GDPR) in the European Union and national data protection laws. These legal acts aim to ensure that personal data is processed lawfully and in a manner that protects individuals' rights and freedoms.

Definition of Personal Data, Their Types, and Special Categories
Personal data refers to any information relating to an identified or identifiable natural person. This can include information such as name, address, social security number, email address, as well as more sensitive data such as health information, sexual orientation, or political opinions. Special categories of personal data, also known as sensitive data, include information that can harm an individual's privacy and are therefore subject to special legal protection.

Principles of Processing "Sensitive" and "Ordinary" Personal Data
The processing of personal data must comply with specific principles, such as:

Lawfulness: Data processing must have a legal basis.
Purpose Limitation: Data should be collected for specific, explicit, and legitimate purposes.
Data Minimization: The processed data must be adequate, relevant, and limited to what is necessary.
Accuracy: Data must be accurate and, where necessary, kept up to date.
Integrity and Confidentiality: Data must be processed in a manner that ensures appropriate security.
"Ordinary" data can be processed based on the consent of the individual or other legal grounds, such as the performance of a contract or legal obligation. "Sensitive" data can only be processed in exceptional cases, such as explicit consent from the individual or the necessity to protect the individual's vital interests.

Data Processing Delegation vs. Data Sharing
Data processing delegation involves transferring personal data to another entity that processes the data on behalf of the data controller. Data sharing refers to the transfer of personal data to another entity that becomes a separate data controller. Delegating data processing requires a delegation agreement that sets the terms and conditions for data processing by the processor.

Rights of Individuals Whose Data Is Processed
Individuals whose data is processed have several rights, including:

Right to Information: The right to know how their data is being processed.
Right of Access: The right to obtain a copy of their data.
Right to Rectification: The right to correct inaccurate data.
Right to Erasure (Right to Be Forgotten): The right to request data deletion in certain circumstances.
Right to Restriction of Processing: The right to restrict data processing in specific situations.
Right to Data Portability: The right to transfer data to another controller.
Right to Object: The right to object to data processing under certain conditions.
The data controller is obliged to ensure the possibility of exercising these rights.

Obligations of the Data Controller and Data Processor
The data controller is responsible for ensuring that data processing complies with legal regulations, including implementing appropriate technical and organizational measures for data protection. The data processor must process data only on the controller's instructions. Both entities must maintain a record of processing activities and report data breaches to the supervisory authority and, in some cases, to the affected individuals.

Appointment, Status, and Tasks of a Data Protection Officer
A Data Protection Officer (DPO) is responsible for overseeing compliance with data protection regulations within an organization. The DPO monitors compliance, advises on data protection matters, trains staff, conducts audits, cooperates with the supervisory authority, and serves as a contact point for individuals whose data is processed.

Ensuring Compliance and Documentation of Data Protection
Ensuring compliance with data protection regulations requires maintaining appropriate documentation, such as data protection policies, processing procedures, records of processing activities, and risk assessments. Organizations must also conduct regular audits and staff training on data protection.

Risk Assessment
Risk assessment is the process of identifying and analyzing potential threats to the security of personal data and implementing measures to mitigate these risks. Risk assessment helps organizations understand the most significant threats to data protection and determine the actions needed to ensure an adequate level of security.

Exercises
Case Study - Personal Data Processing Processes in a Company
Exercises in the form of a case study involve the analysis and evaluation of personal data processing processes in a specific company. Participants become acquainted with the practical aspects of data processing, identify potential problems, and propose solutions in compliance with data protection regulations. The analysis covers the entire life cycle of personal data, from collection, through storage, to deletion.

Types of Documents Related to Selected Data Processing Processes in a Company
These exercises focus on various types of documents essential for the proper management of personal data processing processes in a company. Participants learn to create and manage documentation, which includes:

Contract for Work/Contract for Services: Documents regulating cooperation with external contractors, which may include clauses regarding personal data processing.
Data Processing Agreement: Agreements between the data controller and the data processor, outlining the terms and conditions for data processing on behalf of the controller.
Consent for Image Use: Documents allowing the company to legally use the images of employees or clients for marketing or promotional purposes.
Processing of Ordinary and Sensitive Data: Procedures and policies regarding the differences in processing ordinary data (e.g., name, address) and sensitive data (e.g., health information, biometric data).
Personal Data Protection in the Workplace
Exercises include the analysis of policies and procedures concerning the protection of employees' personal data in the workplace. Participants learn how companies should manage employees' personal data, what security measures to implement, and what rights employees have concerning the protection of their personal data.

Protection and Security of Personal Data from the Perspective of Individuals and Legal Entities, Considering the Challenges of the Digital World

Teaching methods

Lecture: informative presentation, discussion with problem solving.
The lecture is conducted using distance learning techniques in a synchronous mode.
Acceptable platforms: eMeeting, Zoom, Microsoft Teams.
Exercises: discussion with multimedia presentation, case method, discussion.

Bibliography

Basic:
1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483 ze zm.)
2. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
3. Ustawa o ochronie danych osobowychz dnia 10 maja 2018 r. (Dz. U. z 2019 r. poz. 1781 t.j.)
4. Ustawa Kodeks pracy z dnia 26 czerwca 1974 r. (Dz. U. z 2020 r. poz. 1320 t.j.)
5. Fajgielski P. (2019), Prawo ochrony danych osobowych. Zarys wykładu, Wydawnictwo Wolters Kluwer, Warszawa.

Additional:
1. Ustawa Kodeks cywilny z dnia 23 kwietnia 1964 r. (Dz. U. 2020 r. poz. 1740 t.j.)
2. Ustawa o prawie autorskim i prawach pokrewnych z dnia 4 02 1994 r. (Dz. U. 2021 r. poz. 1062 t.j.)
3. Ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2020 r. (Dz. U. 2020 r. poz. 344 t.j.)
4. Majchrzak J., Goliński M., Matura W., The concept of the qualitology and grey system theory application in marketing information quality cognition and assessment, Central European Journal of Operations Research, 2020, Vol. 28, No. 2

Breakdown of average student's workload

	Hours	ECTS
Total workload	50	2,00
Classes requiring direct contact with the teacher	30	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	20	0,50