Data Protection Impact Assessment (DPIA)

Personal Data of Participants in the Online Skills Assessment Questionnaire

DOCUMENT

Document owner	Example University
Legal department	
Informatics	
Business processes	
External collaborators	Tamara Bubnjar, Master of Laws, University of Maribor
Data protection officer	

CONFIDENTIALITY AND COPYRIGHT

Table of Content

Introduction

Example University is the central public institution and institution for adult education in the Republic of Slovenia, established by the Decree of Establishment on 27 September 1991.

The Example University also works in the field of adult education in accordance with the Resolution on the National Education Program in the Republic of Slovenia (2013-2020) and other national and European strategic documents and development guidelines in adult education. The competencies and responsibilities of the Example University are also determined by legal regulations in education, especially the Act on the Organization and Financing of Education Act and the Adult Education Act (2018).

Every year, the Example University prepares and implements more than 40 educational programs for about 800 participants (adults). The basis for the successful involvement of participants in the programs is research and development projects that resonate in the domestic and international environment. Example University aims to increase access to education for learning disadvantaged adults. In doing so, the Example University develops a foundation to support learning (as well as counselling and evaluation) and is constantly upgrading the quality of its educational programs. It contributes to the spread of awareness of the accessibility and importance of lifelong learning and non-formally acquired knowledge, which increase the individuals' quality of life and improve society as a whole.

Due to the complexity and a large number of applications for education, Example University conducted a comprehensive DPIA analysis to reduce the likelihood of risks associated with the protection of personal or sensitive data.

The entire DPIA analysis is performed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR). The basis for the DPIA analysis is also in the List of Personal Data Processing Actions Required to Perform a Personal Data Protection Impact Assessment under Article 35 (4) of the GDPR published by the Information Commissioner, due to the possibility of processing, which in the decision-making process with legal or similarly significant effects include a systematic and extensive evaluation of personal aspects relating to natural persons.

General provisions

For the purpose of validating the results, the impact assessment also includes a self-assessment of compliance with the Information Commissioner's Data Protection Impact Assessment Guidelines version 1.1 and the Data Protection Officers Guidelines of the Data Protection Working Party under Article 29 16/SL WP 243 rev. 01, which confirmed the adequacy of the chosen methodology, the scope and content of the performed assessment of the impact on privacy.

Example University unifies the processing of personal data in the process of project implementation within Example University, which relate directly to the individual and in terms of providing minimum or uniform levels of organisational and technical measures for personal data protection to the Example University since that is its obligation.

Relations and definitions

Glossary of Terms

Personal data: any information relating to an identified or identifiable natural person (i.e., 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.

Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor: a natural or legal person, public authority, agency or another body which processes personal data on behalf of the controller.

Processing: 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.

Recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be

regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Third party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Subprocessor: is a third-party data processor who has or potentially will have access to or process protected data.

Personal data breach: 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.

Supervisory authority: an independent public authority that is established by a Member State pursuant to Article 51. Namely:

> *Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this regulation in order to protect the fundamental rights and freedoms of natural persons in relation to the processing and to facilitate the free flow of personal data within the Union ('supervisory authority').*
>
> *Each supervisory authority shall contribute to the consistent application of this regulation throughout the Union. For that purpose, the supervisory authorities shall cooperate with each other and the Commission*.

cross-border processing means either:

processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the European Union where the controller or processor is established in more than one Member State, or

processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the European Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

Processing of personal data for performance Online Skills Assessment Questionnaire

The reason for carrying out an impact assessment in relation to the protection of personal data

WHY IS IT NECESSARY TO CARRY OUT AN IMPACT ASSESSMENT REGARDING PERSONAL DATA?
In order to evaluate the skills of adults in order to raise their competencies, Example Univerity will implement the Online Skills Assessment Questionnaire (OSAQ). OSAQ is a tool for assessing adult skills. Example University wants to enable adults to evaluate their skills with the OSAQ, and to encourage them to make a personal plan to improve their skills and/or further careers, independently or with qualified professionals, through the assessment of OSAQ skills. Due to the complexity of the OSAQ, the large number of adult participants and Faculties that are part of the university, which will establish direct contact with adult participants, the reason for conducting a data protection impact assessment is to reduce the likelihood of risks related to personal data protection. The analysis focuses on the risks associated with the key processes of personal data processing when conducting assessments with the OSAQ. Given the need to establish a basic framework for personal data management and to determine the relationships in terms of Example University rights and obligations in the processing of personal data, the analysis focuses on personal data obtained in the assessment with the OSAQ.

A detailed description of the data processing method

Nature, context and purpose

DESCRIPTION OF THE NATURE OF THE DATA PROCESSING METHOD
The processing of personal data is divided into four sub-processes: 1. Inviting participants to the evaluation by professionals at Faculties. 2. Acquisition of an Entry Number (EN) from a professional: A) in person in a controlled support environment at Faculties, or B) via e-mail, SMS-message or telephone call, the participant first obtains a token number from the professionals at Faculties and with it obtains the EN online. 3. Professional support while filling out OSAQ at Faculties or from home (professionals supervise the process over the OSAQ application). 4. Access to the reports on the results after the completion of the OSAQ enabled by the EN. The OSAQ application supports three models of performing skill assessment with the OSAQ instrument. It applies for all three models that adult participants can obtain the EN exclusively through direct contact with professionals at Faculties. In the OSAQ implementation model, through controlled support environments, participants receive EN in person at permanent and temporarily operating local OSAQ points, where they also perform assessments. The professional assigns the EN to the participant in person at the Faculties via the OSAQ application. In this case, the professional sees the EN only when printing it on paper or in PDF format. In the OSAQ implementation model, where the filling out takes place from home i.e., in an uncontrolled open environment, the participants receive a token for obtaining the EN via e-mail, SMS or via phone call, and the skills are assessed from home. In this case, the professional does not see the EN. Professionals at Faculties monitor the course of assessment and the status of EN (not the results of assessment) through the OSAQ application and offer participants professional assistance during the completion of the questionnaire if they request it. An adult participant who, after completing the assessment, wishes to attend counselling on the interpretation of the results achieved and counselling regarding the choice of career path

or curriculum may give consent to the selected professional at Faculties to access personal and sensitive data and provide their result reports for each questionnaire module.

THE CONTEXT OF PERSONAL DATA PROCESSING

Example University collects and processes personal data for the purpose of implementing the OSAQ on the basis of point a. Paragraph 1 of Article 6 of the GDPR, namely: the data subject has consented to the processing of his personal data for one or more specific purposes and on the basis of Article 8 of ZVOP-1 (Slovenian law), which stipulates that personal data may only be processed if the processing of personal data and the personal data being processed are provided for by law or if the personal consent of the individual has been given for the processing of certain personal data.

The second paragraph of Article 8 of ZVOP-1 stipulates that the purpose of personal data processing must be determined by law, and in the case of processing based on the personal consent of the individual, the individual must be previously informed in writing or in another appropriate manner of the personal data processing purpose. In view of the above, individuals can reasonably expect that personal data will be used in the manner and for the purpose as described.

WHAT IS THE PURPOSE FOR COLLECTING DATA?

Data are collected for the purpose of implementing the OSAQ in the Example University, which is a tool for assessing adult skills. The purpose of the OSAQ is to enable adult participants to evaluate their skills and, based on the results, structure their education, raise their competencies and improve their further careers.

ARRANGEMENT OF RELATIONS BETWEEN CONTROLLER AND PROCESSOR

In order to perform the analysis from the point of view of the provisions of the GDPR, three essential distinguishing elements between the controller and the processor must be taken into account in order to identify the stakeholders of individual personal data processing (in accordance with data commissioner practice). The role of the processor will be performed by the legal or natural person who will process personal data (1) exclusively in the name and on behalf of the personal data controller, (2) draw the basis for personal data processing from the controller's rights and (3) in relation to the processing operations themselves, be bound by the instructions of the controller.

In the specific case, in order to meet the goals of OSAQ, Example University organized Faculties that collect personal data of adult participants for the needs of Example University. Faculties are therefore processors of personal data. Namely, the faculties do not collect personal data in their own name and for their own account, but in the name and for the account of Example University.

TRANSFER OF DATA TO THIRD COUNTRIES

The transfer of data to third countries is not required, but the prohibition of data transfer to third countries is not explicitly regulated by a contract or other mechanism.

Personal data processing

NO.	DATA	MANDATORY	LEGAL GROUNDS	ACCESS TO DATA	STORAGE PERIOD
1.	First and last name of the adult	Yes	Consent of a data subject	Professional staff	2 years
2.	Unique identification number	Yes	Consent of a data subject	Professional staff	2 years
3.	Registration number	Yes	Consent of a data subject	Professional staff	2 years
4.	Date and place of birth	Yes	Consent of a data subject	Professional staff	2 years
5.	State of birth	Yes	Consent of a data subject	Professional staff	2 years
6.	Citizenship	Yes	Consent of a data subject	Professional staff	2 years
7.	Permanent residence	Yes	Consent of a data subject	Professional staff	2 years
8.	Telephone number	Yes	Consent of a data subject	Professional staff	2 years
9.	E-mail address	Yes	Consent of a data subject	Professional staff	2 years
10.	Formal education	Yes	Consent of a data subject	Professional staff	2 years
11.	Profession	Yes	Consent of a data subject	Professional stff	2 years
12.	Employment status	Yes	Consent of a data subject	Professional staff	2 years
13.	Entry number	Yes	Consent of a data subject	Professional staff	2 years
14.	Employment status	Yes	Consent of a data subject	Professional staff	2 years
15.	Previously completed educations	Yes	Consent of a data subject	Professional staff	2 years

Levels of compliance

Level	Description of compliance level	Measures
HIGH	The information is unlikely to be relevant or its processing probably does not represent proportionate processing of personal data. In cases where the information is not specified in the regulations, when the purpose or type of processing may be questionable in relation to the regulations and where the information is probably not necessary to achieve the purpose of the processing.	Finding alternative data processing solutions. Interruption of data collection and processing.
MEDIUM	The information is probably relevant, and its processing is likely to constitute proportionate processing of personal data according to the purpose of the processing. In cases where the processing of personal data is indirectly or unclearly determined by law, in the case of open definitions of the content of the data in the regulations and in cases where the data is not essential in all respects to achieve the purpose of the processing (e.g., the purpose of processing can be achieved but with more effort).	Particular care in examining and validating the analysis. Relevance and proportionality should be analysed by several experts, if necessary, in the form of a workshop. When reviewing an analysis, a DPO review is required when appointed.
LOW	The information is no doubt proportionate and relevant to the processing of personal data. In cases where the processing of personal data is explicitly and unambiguously allowed by the regulations and where it is indisputable (it is obvious) that the essential goals of the processing cannot be achieved without this data.	No additional action is needed.
N/A	Information in a certain table cell is not provided because it does not apply to a particular case in question.	No additional action is needed.

Necessity and proportionality assessment

LEGAL BASIS FOR DATA PROCESSING
The legal basis for processing personal data is compliance with a legal obligation to which the controller is subject, namely, according to point (a) of paragraph 1 of Article 6 of the GDPR and Article 8 ZVOP-1 (Slovenian law).

OTHER METHODS WITH A LOWER LEVEL OF VIOLATION OF THE RIGHT TO PRIVACY
Other methods were not considered. The data controller has clearly stated and described the reason, purpose and goal of the data processing. Data processing is carried out with the consent of the data subject. The controller collects and processes only the personal data specified by the regulations, and therefore, taking into account that the legislator took into account the necessity and

proportionality of processing actions in relation to the purpose, the processing is necessary and proportionate to the purpose of conducting adult skills assessment using the OSAQ online questionnaire.

IS DATA PROCESSED FOR OTHER PURPOSES?
Given the legal basis for the processing of personal data, Example University has no basis to process personal data outside the purpose, scope or types of processing specified by law. This does not mean that Example University is restricted from processing personal data for other purposes if it has an appropriate basis to do so (e.g., consent of the data subject or contract).

INFORMING INDIVIDUALS ABOUT DATA PROCESSING
The data subject may become acquainted with the conditions of personal data processing and his or her rights regarding the processing in publicly available privacy statements. Example University describes in detail which personal data it processes and for what purpose.

Security measures

DATA PROTECTION MECHANISMS
Only members of the Faculties team and the IT solutions administrator at Example University have access to the Intranet Example University, using a username and password.

DATA INTEGRITY PROTECTION MECHANISMS
All personal data collected is stored and archived in a secure manner. The places where the holders of the protected personal data are located (any document on which personal data is recorded and any other computer or electronic data carrier) and hardware and software (hereinafter referred to as 'protected spaces') shall be protected by organisational, physical and technical measures which prevent unauthorised persons from accessing the data (e.g. lock protection, security systems, alarm systems, video surveillance).

Computers or other hardware on which personal data is processed or stored are turned off and physically or programmatically locked outside working hours, and access to personal data stored on your computer's disk is encrypted with a password.

The keys to the places where the personal data carriers and computer equipment are stored shall be kept by any employee, or the Example University authorised person with due diligence as in their own affairs and in particular by denying access to the key to unauthorised persons.

MECHANISMS FOR DATA LOSS PREVENTION

The controller has a backup system that is used to back up collections of personal data.

Records of personal data processing activities are also kept, but access to them is limited. The storage of documents with personal data is carried out in accordance with applicable legal regulations. The storage of documents containing personal data is carried out in accordance with applicable legal regulations.

LIABILITY OF THE PERSONS PROCESSING PERSONAL DATA

Professionals will sign a "Data Protection Statement" stating:

1. that they will not disseminate and transfer the contents and methodologies of the OSAQ to unauthorized persons, or otherwise affect the validity and reliability of data obtained with a standardized instrument
2. that they are familiar with the nature of the data collected and the data regarding the results of the skills assessment owned by the individual who completed the assessment. Data and results will be protected as confidential in accordance with the Personal Data Protection Act and the General Data Protection Regulation (Regulation (EU) 2016/679, OJ L 119)
3. that they will not disclose the data to other unauthorized persons or use them in any way for purposes other than those specified in the ESS project Professional Support in the Field of Acquisition of Core Competences 2016-2022
4. that they will provide access to the entry number exclusively to individuals who will participate in the assessment according to the envisaged protocol

5. that they will be able to access the results of the assessment only with the written consent of the individual, for the purposes set out in the ESS project Professional Support in the Field of Acquisition of Core Competences 2016-2022.

that they will use exclusively anonymized analyzes of the skill status of adults who have completed the assessment in our organization and are carried out on samples that ensure anonymity to the individual.

Detailed risk assessment

Risk assessment methodology for the rights and freedoms of data subjects

In order not to overlook the essential requirements of regulations, guidelines and good practices, we followed a systematic and objectified approach to assessing risks for the rights and freedoms of data subjects.

After reviewing the relevant literature, we decided to base the approach on the ISACA guidelines, which were developed with the purpose of unifying several different bases for ensuring privacy, namely:

- GDPR,
- ISO/IEC 29100:2011, Information technology – Security techniques – Privacy framework (which has not yet been adopted as a Slovenian standard SIST),
- Asia-Pacific Economic Cooperation (APEC) Privacy Framework,
- Generally Accepted Privacy Principles (GAPP), developed jointly by AICPA, ISACA in IIA.

ISACA PRIVACY PRINCIPLES
1. Choice and consent 2. Legitimate purpose specification and use limitation 3. Personal information and sensitive information life cycle 4. Accuracy and quality 5. Openness, transparency and notice 6. Individual participation 7. Accountability 8. Security safeguards 9. Monitoring, measuring, reporting 10. Preventing harm 11. Supplier / third party management 12. Breach management

13. Security and privacy by design
14. Free flow of information and legitimate restriction

On the basis of the analysis carried out, the controller concludes that he collects and processes exclusively those personal data which are provided for by consent of a data subject and the regulations and, therefore, taking into account that the legislature has taken into account the necessity and proportionality of the processing operations according to the purpose, the processing subject to the analysis is necessary and proportionate to the purpose of the OSAQ.

Risk assessment for the rights and freedoms of data subjects, where the Example University is the controller and Faculties are processors.

		BEFORE MEASURES					AFTER MEASURES		
Nr.	RISK	PROBABILITY	SEVERITY	RISK	NOTES	MEASURE	PROBABILITY	SEVERITY	RISK
COMULATIVE VALUE				**high**					**medium**
1	**Choice and consent**			**high**					**low**
1	There is no legal basis for processing	low	high	medium	Through thorough analysis, we found that the processing, the purpose and the types of personal data are determined by the consent of a data subject	Signing a contract for processing and control	low	medium	low
2	The legal basis is not properly selected	low	high	medium	Example University obtain explicit consent from a data subject by offering an explicit consent screen that contains Yes and No check boxes, and text that clearly indicates the consent	Signing a contract for processing and control	low	medium	low
3	Use of legitimate interest by public authorities in the performance of their tasks	high	high	high	We use a legitimate interest	Signing a contract for processing and control	low	medium	low
4	The conditions for consent are not clear	medium	high	high	The conditions for consent are clear and transparent	Signing a contract for processing and control	low	medium	low
5	The terms of consent are not separated by purpose	high	high	high	The terms of consent are separated by purpose	Signing a contract for processing and control	low	medium	low
6	An individual is unlawfully coerced into consent in an incompatible	low	high	medium	An individual is not coerced into consent.	Signing a contract for processing and control	low	low	low

	relationship with another lawful ground							
7	Consent is not clearly different from other matters	medium	high	high	Consent is clearly different from other matters	Signing a contract for processing and control	low	medium	low
8	Consent is not in clear and simple language	medium	high	high	Consent is clear and is written in a language understandable to adults	Signing a contract for processing and control	low	low	low
9	The consent may not be revoked at any time by an individual	high	high	high	Individuals can revoke consent on a prepared form	Signing a contract for processing and control	low	medium	low
10	Consent is not as easy to revoke as to give	high	high	high	Individuals can revoke consent on a prepared form	Signing a contract for processing and control	low	medium	low
11	Consent for children has not been obtained from holders of parental rights	low	high	medium	Children do not participate in the assessment because participants are exclusively adults	Signing a contract for processing and control	low	low	low
12	Risks related to the processing of children's personal data	low	high	medium	Children do not participate in the assessment because participants are exclusively adults	Signing a contract for processing and control	low	low	low
2	**Legitimate purpose specification and use limitation**			**high**					**low**
13	The purpose of the processing is not specified	medium	medium	medium	The purpose of the processing was clearly defined	Signing a contract for processing and control	low	low	low
14	The purpose of the processing is not explicit or clearly defined	medium	medium	medium	The purpose of processing is clear and it refers to only one purpose of processing	Signing a contract for processing and control	low	low	low
15	The purpose of the processing is not legal	medium	high	high	Through thorough analysis, we confirmed that the purpose of the processing was lawful	Signing a contract for processing and control	low	medium	low
16	The retention period is not set	low	high	medium	The storage period has been precisely defined	Compliance with storage period	low	low	low
17	Use of data for another purpose than the purpose for which it was collected	low	high	medium	We guarantee the use of personal data only for a defined purpose, which are defined in OSAQ	Signing a contract for processing and control	low	low	low
18	Excessive data volume for processing (minimum data volume not used)	low	high	medium	Through thorough analysis, we found that we only process data given by the consent of a data subject	Signing a contract for processing and control	low	medium	low
19	Retention period exceeded	medium	high	high	after the retention period, the data is destroyed	Signing a contract for processing and control	low	medium	low

20	The processing method does not guarantee the security of personal data	medium	medium	medium	We control the processing method	Signing a contract for processing and control	low	medium	low
21	There is no protection against tampering or illegal processing	medium	high	high	We control the processing method	Signing a contract for processing and control	low	medium	low
22	There is no protection against unintentional loss or destruction of personal data	low	high	medium	We control the processing method, data is mostly originally in paper form	Signing a contract for processing and control	low	medium	low
23	There is no protection against accidental data corruption	low	high	medium	We control the processing method, the data are mostly originally in paper form	Signing a contract for processing and control	low	medium	low
24	Risks related to automated decision making	low	high	medium	We do not make automated decisions	Signing a contract for processing and control	low	medium	low
25	Risks related to profiling	low	high	medium	We do not design profiles	Signing a contract for processing and control	low	low	low
26	Different ages of consent between Member States have not been considered	low	high	medium	OSAQ is only for Slovenian citizens	Signing a contract for processing and control	low	medium	low
27	Processing special categories of personal data without meeting any of the specific conditions in Article 9 of the GDPR	low	high	medium	We do not process special categories of personal data	Signing a contract for processing and control	low	medium	low
3	**Personal information and sensitive information life cycle**			**high**					**medium**
28	Extension of retention period with no legal basis	low	high	medium	The storage period is 2 years, after which the data are destroyed	Signing a contract for processing and control	low	medium	low
29	Failure to extend the retention period, where there is a legal basis or at the request of the individual	medium	high	high	The storage period is 2 years	Signing a contract for processing and control	low	medium	low
30	Undefined procedures of the individual's	medium	high	high	We manage risk with a pre-prepared form	Pre-prepared form that	low	medium	low

	request after verification if the controller processes data					the individual participants only fill out			
31	Undefined procedures of the individual's request for access to data processed by the controller	medium	high	high	We manage risk with a pre-prepared form	Pre-prepared form that the individual participants only fill out	low	medium	low
32	Undefined procedures for individual's requests after restriction of processing	medium	high	high	We manage risk with pre-prepared forms	Pre-prepared form that the individual participants only fill out	low	medium	low
33	Undefined procedures for individual's requests after data deletion	medium	high	high	We do not control the processes at Faculties	Signing a contract for processing and control	low	medium	low
34	Undefined procedures of the individual's request for data portability	medium	high	high	A data subject give a clear consent for data portability	Pre-prepared form that the individual participants only fill out	low	medium	low
35	Undefined procedures in case of an individual's objection	medium	high	high	The process is defined in Data Protection Policy	Data Protection Policy	low	medium	low
36	Improper implementation of procedures in case of an individual's request to verify that the controller is processing data	high	high	high	The process is defined in Data Protection Policy	Data Protection Policy	low	medium	low
37	Improper implementation of procedures in case of individual's request access data processed by the controller	high	high	high	The process is defined in Data Protection Policy	Data Protection Policy	low	medium	low
38	Improper implementation of procedures in case of an individual's request for restri ction of processing	high	high	high	The process is defined in Data Protection Policy	Data Protection Policy	low	medium	low
39	Improper implementation of procedures in case of an individual's	high	high	high	The process is defined in Data Protection Policy	Data Protection Policy	low	medium	low

	request for deletion of data								
40	Improper implementation of procedures in case of an individual's request for data portability	medium	high	high	The process is defined in Data Protection Policy	Data Protection Policy	N/A	medium	low
41	Improper implementation of procedures in case of the objection of an individual	high	high	high	The process is defined in Data Protection Policy	Data Protection Policy	low	medium	low
42	Unnecessary processing of special categories of personal data	low	high	medium	We do not process special categories of personal data	Data Protection Policy	low	high	medium
43	The implementation of information systems and the design of processes do not take into account data protection by default and by design	high	high	high		Signing a contract for processing and control, Design of good practices	medium	medium	medium
44	No data protection impact assessment has been produced	low	high	medium		Implementation of the DPIA	low	medium	low
4 Accuracy and quality				**high**					**medium**
45	The information is incorrect	medium	high	high	The procedure for data processing is defined in the data protection policy	Upgrade a Data Protection Policy	low	low	low
46	An individual's data is not updated when the individual changes it	low	high	medium	The procedure for data processing is defined in the data protection policy and the data is regularly updated	Upgrade a data protection policy	low	medium	low
47	In the case of data change, not all data of the individual is updated	high	high	high	The procedure for data processing is defined in the data protection policy and the data is regularly updated	Upgrade a data protection policy	medium	medium	medium
48	Undefined procedures in case of an individual's request for rectification of data processed by the controller	high	high	high	We manage risk with pre-prepared forms	Pre-prepared form that the individual fills out	low	medium	low
49	Improper implementation of procedures when requesting an individual to	medium	high	high	The procedure for data processing is defined in the data protection policy	Upgrade a data protection policy	low	medium	low

	correct data processed by the controller							
5	**Openness, transparency and notice**			**high**				**medium**
50	The information is not transparent to the individual	medium	high	high	The existing privacy statement clearly shows the bases, data sets, purposes and related retention periods.	Data protection policy	low	medium	low
51	The information is provided in a way adjusted for children.	N/A	high	low	The information is provided in the usual way	Data protection privacy	N/A	medium	low
52	Information presented to the individual is not uniform for all controllers and processors	medium	high	high	It is evident from the existing privacy statements that the information is uniform	Data protection policy	medium	low	low
53	Ways to exercise the rights of the individual are not given in a comprehensive and clear manner	high	high	high	It is evident from the existing privacy statement that they give out comprehensive instructions	Upgrade a data protection policy	medium	medium	medium
54	Information is not provided to an individual when obtaining personal data	high	high	high	The OSAQ does not include an attachment with a privacy statement	Supplement the OSAQ with a privacy statement	low	medium	low
55	Inaccurate informing of an individual when information is not obtained from an individual	low	high	medium	There is no established practice of collecting data from third sources, so no statement has been made for data subjects	Data protection policy	low	low	low
6	**Individual participation**			**high**				**low**
56	The portable data received by an individual are not machine-readable	medium	high	high	The portsable data are clear and machine-readable.		low	medium	low
57	The portable data received by an individual is incomplete	medium	high	high	The portable data is complete and clear		low	medium	low
58	The decision made by automatic decision-making is final	medium	high	high	We do not use automated decision making		low	low	low
59	Automatic listing of an individual's is definitive	medium	high	high	We do not use profiling		low	low	low
60	For the joint controllers, the agreement does not clearly set out all the rights	N/A	high	low	We are not joint controllers		N/A	high	low

	and obligations of each of the controllers							
61	The content of the joint controller's agreement is not accessible to the individual	N/A	high	low	We are not joint controllers		N/A	high	low
62	There is no designated contact point for the individual	low	high	medium	We designated contact point for the individual	Publicly published contact data (on the website)	low	low	low
63	The contract unlawfully restricts the exercise of individual rights to certain controllers	N/A	high	low	We are not joint controllers		N/A	high	low
64	There is no designated data protection authority	medium	high	high	We have named a DPO	Signing a contract for processing and control	low	medium	low
65	The contact details of the Data Protection Officer are not accessible to the individual	low	high	medium	We have published the DPO's contact information	Signing a contract for processing and control	low	low	low
7	**Accountability**			**high**					**low**
66	There is no defined procedure for determining whether the processing of personal data for other purposes is legal	medium	high	high	The Example University does not process data for other purposes	Signing a contract for processing and control	low	low	low
67	The tasks and responsibilities of the Data Protection Officer are not clearly defined	low	high	medium	We have defined the DPO's tasks and responsibilities	Signing a contract for processing and control	low	medium	low
68	There is no defined procedure for consulting the supervisory authority in light of the results of the privacy impact analysis	medium	high	high	The DPO shall forward requests for an opinion to the supervisory authority or, in the ex-ante advice procedure, forward the impact assessment to the supervisory authority.	Signing a contract for processing and control	low	medium	low
8	**Security safeguards**			**high**					**low**
69	There are no documented security policies for protecting personal information	low	high	medium	We have our own security policies and risk assessment	Data protection policy	Low	medium	low

70	There is no documentation of personal data processing for purposes other than the purpose for which they were collected	medium	high	high	The Example University does not process data for other purposes	Data protection policy	low	medium	low
71	Organisational measures for the protection of personal data are not clearly defined	low	high	medium	We have our own security policies and risk assessment	Data protection policy	low	low	low
72	There are no clearly defined technical measures for the protection of personal data	low	high	medium	We have our own security policies and risk assessment	Data protection policy	low	medium	low
73	Organisational measures to protect personal data are not sufficient	medium	high	high	We have our own security policies and risk assessment	Data protection policy	low	medium	low
74	Technical measures to protect personal data are not sufficient	low	high	medium	We have security policies and high technical standards	Data protection policy	low	medium	low
75	Organisational measures to protect personal data are not being implemented	low	high	medium	We have our own security policies and risk assessment	Data protection policy	low	medium	low
76	No technical measures are in place to protect personal data	medium	high	high	We have our own security policies and risk assessment	Data protection policy	low	medium	low
77	There is no regular check on security controls	medium	high	high	We have our own security policies and verification procedures	Data protection policy	low	medium	low
78	Organisational controls for the protection of personal data are not clearly defined in contracts with processors	high	high	high	We have a data processing contract, where organizational controls are clearly defined	Data protection policy	low	medium	low
79	Technical control contracts for the protection of personal data are not clearly defined in contracts with processors	high	high	high	We have a data processing contract where organizational controls are clearly defined	Agreed on a contract for processing and control	low	medium	low

9	**Monitoring, measuring, reporting**			**high**				**medium**
80	The Data Protection Officer does not guarantee the implementation of privacy impact assessments	medium	high	high	We perform impact assessments	Implemented an annual tasks plan for the DPO	low	medium	low
81	The Data Protection Officer does not check compliance with the regulations	medium	high	high	We perform compliance checks, also with DPIA	Signing annual tasks plan for the DPO	low	low	low
82	The Data Protection Officer does not educate employees	low	high	medium	We educate, train and inform our employees	Implemented an annual tasks plan for the DPO	low	medium	low
83	The Data Protection Officer does not cooperate with the supervisory authority	low	high	medium	The DPO cooperates with the supervisory authority (DPO sends requests for an opinion or, in the ex-ante advisory procedure, forwards the impact assessment)	Implemented an annual tasks plan for the DPO	low	low	low
84	No reporting regarding the correction of personal data is introduced	medium	high	high	Faculties does not report any corrections of personal data	Signing a contract for processing and control	medium	medium	medium
85	No reporting regarding the deletion of personal data is introduced	medium	high	high	Faculties does not report the deletion of personal data	Signing a contract for processing and control	medium	medium	medium
86	There is no documented content reporting on an individual's personal information	medium	high	high	Faculties does not documented reporting on an individual's personal information	Signing a contract for processing and control	low	medium	low
87	Reporting on the transfer of individual data to third parties is not introduced	low	high	medium	Example University is the only controller	Signing a contract for processing and control	low	medium	low
88	Copies of personal data provided as part of the right to data portability have been preserved longer than the retention period	medium	high	high	.The storage period is 2 years, then the copies of personal data are destroyed		low	medium	low
89	No triggers have been identified to produce a privacy impact analysis	medium	high	high	Example University shall comply with the rules laid down by the regulations and reevaluate the impact in case changes to the legal basis or		low	medium	low

				processing of new personal data.				
90	There are no policies in place to design and maintain records of processing activities	low	high	medium	We carry out our activities in accordance with the instructions of our DPO	Implemented an annual tasks plan for the DPO	low	medium	low
91	Recipients of personal data are not identified	low	high	medium	Each request requires identification of individual	Data protection policy	low	medium	low
10	**Preventing harm**			**high**					**medium**
92	Guidelines for determining the legality of processing have not been established	low	high	medium	We use EDPB's guidelines as well as those from the information commissioner	Data protection policy	low	medium	low
93	No consequences are determined for the individual in case of further processing of personal data	medium	high	high	We do not further process personal data	Data protection policy	low	medium	low
94	There is no adequate safeguard for decision making based on special categories of personal data	low	high	medium	We do not process special categories of personal data	Data protection policy	low	medium	low
95	There is no guarantee that the exercise of an individual's right will not adversely affect the rights and freedoms of others	high	high	high	We exercise the rights of the data subjects only in accordance with the law, so we have no direct influence on any negative impact and potential negative impacts require a change in regulations.	Data protection policy	medium	medium	medium
96	Pseudonymised personal data is not considered personal data	medium	high	high	We do not use a pseudonymized personal data	Data protection policy	low	medium	low
97	No rules and procedures have been put in place to minimise the harm to an individual when archiving in the public interest	N/A	high	low	The process does not include permanent archiving material in the public interest	Signing a contract for processing and control	N/A	medium	low
98	No rules and procedures have been put in place to minimise harm to an individual for use of their personal data in historical and scientific	low	high	medium	For scientific research purposes, we only use anonymised data	Signing a contract for processing and control	low	low	low

	research purposes								
99	No rules and procedures have been put in place to reduce harm to an individual for statistical use of their personal data	low	high	medium	For statistical purposes, we keep aggregated data (rather than anonymised) to reduce the risks associated with inappropriate anonymisation.	Upgrade a data protection policy, signing a contract for processing and control	low	low	low
11	**Supplier / third party management**			**high**					**medium**
100	No outsourcing management policies are in place	low	high	medium	We manage external contractors according to established procedures	Data protection policy, signing a contract for processing and control	low	low	low
101	Outsourcing arrangements do not contain sufficient guarantees that adequate organisational measures are in place to protect personal data	high	high	high	We have an agreement with the faculties on cooperation in the implementation of skills assessment with the help of the OSAQ	Data protection policy	medium	medium	medium
102	Outsourcing arrangements contain sufficient guarantees that adequate technical measures are in place to protect personal data	high	high	high	We have an agreement with the faculties on cooperation in the implementation of skills assessment with the help of the OSAQ	Data protection policy	medium	medium	medium
103	Sufficient restrictions and rules for hiring sub-contractors have not been applied	high	high	high	We have an agreement with the faculties on cooperation in the implementation of skills assessment with the help of the OSAQ	Data protection policy, signing a contract for processing and control	medium	medium	medium
104	Procedures and duration of processing are not specified in the agreement with the processors	high	high	high	We have an agreement with the faculties on cooperation in the implementation of skills assessment with the help of the OSAQ	Data protection policy, signing a contract for processing and control	low	low	low
105	The purpose and type of processing is not specified in the agreement with the processors	high	high	high	We have an agreement with the faculties on cooperation in the implementation of skills assessment with the help of the OSAQ	Data protection policy, signing a contract for processing and control	low	low	low
106	The types of personal data subject to processing are	high	high	high	We have an agreement with the faculties on cooperation in the implementation of skills	Data protection policy, signing a	low	low	low

	not specified in the agreement with the processors				assessment with the help of the OSAQ	contract for processing and control		
107	The types of individuals whose personal data are subject to processing are not specified in the agreement with the processors	high	high	high	We have an agreement with the faculties on cooperation in the implementation of skills assessment with the help of the OSAQ	Data protection policy, signing a contract for processing and control	low	low	low
108	In agreement with the processor, not all 8 obligations are specified as per Article 28 paragraph 3 of the GDPR	medium	high	high	We have an agreement with the faculties on cooperation in the implementation of skills assessment with the help of the OSAQ	Data protection policy, signed a contract for processing and control	low	low	low
109	The agreement with the processor does not specify the obligation and the procedure for reporting incidents	low	high	medium	We have an agreement with the faculties on cooperation in the implementation of skills assessment with the help of the OSAQ	Data protection policy, signed a contract for processing and control	low	medium	low
110	There are no requirements for the processor to outsource his work	high	high	high	We have an agreement with the faculties on cooperation in the implementation of skills assessment with the help of the OSAQ	Data protection policy, signed a contract for processing and control	medium	medium	medium
111	There are no procedures in place to ensure that processors comply with the requirements of the controller	high	high	high	We have an agreement with the faculties on cooperation in the implementation of skills assessment with the help of the OSAQ	Data protection policy, signed a contract for processing and control	low	medium	low
112	There are no procedures in place for the employee of the controller to comply with the requirements of the controller	low	high	medium	Compliance with the requirements of the controller is in the description of the employee's work tasks.	Upgrade Employment contract	low	medium	low
12	**Breach management**			**high**					**low**
113	Procedures for notifying the supervisory authority of incidents have not been established	low	high	medium	The DPO notifies the supervisory authority with the consent of the Example University representative	Implemented annual tasks plan for the DPO	low	medium	low
114	Procedures for notifying individuals of violations are not specified	medium	high	high	The DPO notifies the supervisory authority with the consent of the Example University representative	Implemented annual tasks plan for the DPO	low	medium	low

115	The content of the notice is not specified in accordance with the regulations	medium	high	high	Create a notification template	Design of template for notification	low	medium	low
13	**Security and privacy by design**			**high**					**medium**
116	Privacy and security policies do not respect the rights of the individuals	high	high	high	Devised privacy policies respect and protect the rights of the individuals	Privacy policies	medium	medium	medium
117	Privacy and security policies do not respect the freedoms of the individuals	medium	high	high	Devised privacy policies respect the freedoms of the individuals	Privacy policies	low	medium	low
118	Privacy and security policies do not take into account the legitimate interests of the individuals	medium	high	high	Devised privacy policies take into account the legitimate interests of the individuals	Privacy policies	low	medium	low
119	Automatic procedures (with legal or similarly significant effect on individuals) do not involve manuall human intervention	medium	high	high	Procedures are always supported by manual decision-making, as follows from the published statements on the protection of privacy of the Example University	Data protection policy	low	medium	low
120	No policies have been put in place to assess the nature, extent, context and purposes of the processing of personal data	medium	high	high	Covered as part of the records of processing activities	Data protection policy	low	medium	low
121	An impact assessment on an individual is not an input to the requirements for designing information solutions	medium	high	high	Policies for privacy by design when addressing security aspects of information solutions have not been devised; instead, we use privacy policies	Design of privacy policies	low	medium	low
122	Harm reduction for an individual is not an integral part of the process of creating information solutions	medium	high	high	Policies for privacy by design when addressing security aspects of information solutions have not been devised; instead, we use privacy policies	Design of privacy policies	medium	medium	medium
14	**Free flow of information and legitimate restriction**			**high**					**low**

123	No procedures for validating binding business rules have been defined	medium	medium	medium	We do not use binding corporate rules	Data protection policy	low	low	low
124	No data transfer procedures are defined at the request of other persons	high	high	high	The Example University shall forward the data to other bodies when appropriately requested to do so.	Data protection policy	low	medium	low
125	Data transfer procedures to a third country are not defined	high	high	high	We do not transfer data to third countries	Data protection policy	low	medium	low
126	No data protection procedures are in place for their transmission	medium	high	high	Protection procedures may also depend on the recipient's technical solutions	Data protection policy	low	medium	low

Analysis of risk assessment for the rights and freedoms of data subjects in the case where the Example University is the data controller and Faculties processor.

The risk analysis is based on a higher level of individual risks and focuses on recommendations and solutions.

In doing so, the controller must establish detailed and clear instructions regarding the obligations, which will be taken into account in the context of its information solutions in terms of organisational and technical measures for the protection of personal data.

We found that with the envisaged measures, we can reduce the risk to the rights and freedoms of data subjects to such an extent that we did not assess any risk as "high risk", so that is why, in terms of risks for the data subjects or reducing the damages, this type of arrangement where the Example University is the controller and Faculties are processors, is suitable and appropriate.

RISK GROUP	THE HIGHEST RISK BEFORE MEASURES	THE HIGHEST RISK AFTER MEASURES
1 Choice and consent	high	low
2 Determination of lawful purpose and limitation of use	high	low
3 The life cycle of personal and sensitive information	high	medium
4 Punctuality and quality	high	medium
5 Openness, transparency and information	high	medium
6 Participation of individuals	high	low
7 Responsibility	high	low
8 Security measures	high	low
9 Monitoring, measuring and reporting	high	medium
10 Prevention of damage	high	medium
11 Supplier / third party management	high	medium
12 Management of incidents	high	low
13 Built-in security and privacy	high	medium

14 Free movement of information and legal restriction	high	low

Consultations

WERE REPRESENTATIVES OF THE PARTICIPANTS CONSULTED?
Representatives of the participants were not consulted.

Audit procedure

UPDATING THE IMPACT ASSESSMENT
The impact assessment should be updated regularly, which means each time there is a major change in regulations, business processes, data, purposes or types of personal data processing – once in a year. If changes in the environment have not triggered an update earlier than in three years, it is mandatory to update the impact assessment within three years at the latest.

Conclusion

RESULT ANALYSIS
The DPIA results show that the approach in which Example University is a controller and Faculties processor of personal data is appropriate. The implementation of measures, the essential of which are the signed contract of processing between Example University and Faculties on data processing, control over the personal data, and the introduction of appropriate risk monitoring, will not pose a significant risk to the rights and freedoms of data subjects. A key condition for the proper regulation of contractual relations is the existence of a written processing contract (this can also be concluded in an equivalent electronic form). An integral part of the processing contract must be specified procedures and measures for securing personal data to be held by the processor (the contract must indicate whose data and for what purpose and for how long the processor will process on behalf of the controller, the scope of the controller's rights and obligations with regard to personal data must also be evident, as the controller cannot transfer to the processor more rights than he himself has, and at the same time the restrictions for the controller also constitute restrictions for the processor). Mere references to the requirements of ZVOP-1 or provisions such as “data will

be protected in accordance with ZVOP-1" are not sufficient. Procedures and measures for data security need to be defined and specified (e.g., what are the procedures for physical security, data copying, etc.). It is also permissible to refer to the existing rules on information security of the controller or processor, if of course, these rules are appropriate. For this purpose, Example University also uses privacy statements, which clearly state how personal data is protected (both from a technical point of view and from an organizational point of view). In particular, the Statement states that:

- the content and methodology of the OSAQ online instrument will not be disseminated and forwarded by employees to unauthorized persons, or the validity and reliability of data obtained with a standardized instrument will not be otherwise affected;
- employees are familiar with the nature of the data collected and the results of the skills assessment owned by the individual who completed the assessment. Data and results will be protected as confidential in accordance with ZVOP-1 and GDPR;
- that employees will not disclose the data to other unauthorized persons or use it in any way for purposes other than those specified in theOSAQ;
- employees will provide access to the entry number exclusively to individuals who will participate the assessment according to the planned protocol;
- employees will access the results of the assessment only with written consent from the data subjects for the purposes set out in theOSAQ.