Data Protection Impact Assessment (DPIA)

Personal data of students upon Student enrolment

DOCUMENT

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

CONFIDENTIALITY AND COPYRIGHT

Table of Content

Introduction

Example University is one of the leading educational and research institutions. Example University provides students with knowledge based on internationally recognised scientific research work, enabling them to integrate into future working environments in the international arena successfully.

The long-standing successful operation of the Example University is aimed at consolidating the position of an internationally recognised university education and research institution in different fields, which is of high quality and attractive to students of all levels.

To achieve this objective, Example University implements innovative teaching methods in a modern learning environment. The operation focuses on the student, and the planning of enrolment is socially responsible. In addition to quality and content-rich and topical study programmes, an important place in the activities of the Example University also occupies a research activity that is closely linked to successful pedagogical work. Important elements here are: tracking the latest trends and events in the world about which students can be informed through the study process, further creativity, achievement of internationally comparable scientific research excellence and sustainable, socially responsible and quality development of scientific fields, fields and sub-fields of the University.

The functioning of the University is based, inter alia, on the promotion of academic values, the promotion of comprehensive student personality development, with an emphasis on the active co-design of events at the University and participation in the study activities, the promotion of international mobility of employees and students, the promotion of active activities of the alumni club and programme councils of the fields of study.

Due to the complexity and a large number of student enrolments on Smart Campus, Smart Campus 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 the use of new technologies, processing affects a large number of data subjects, can include monitoring of publicly accessible areas on a large scale, and/or systematic monitoring.

General provisions

The Data Protection Impact Assessment (DPIA) is a document of detailed and thorough risk analysis in the processing of personal data, in this case, the processing of personal data in the implementation of the student's enrolment.

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.

The purpose of the Example University is to unify 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 center, 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

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 the student enrolment procedures

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?
Due to the complexity of the project, a large number of student enrolments in the project, the reason for carrying out an impact assessment in relation to data protection is to reduce the likelihood of risks associated with the protection of personal or sensitive data. The analysis focuses on the risks associated with the key processes of personal data processing in the implementation of student enrolment in the Example University. Given the need to establish a basic framework for personal data management and to determine the relationships in terms of the rights and obligations of the Example University in the processing of personal data, the analysis focuses on personal data obtained by enrolling students in the Example University.

A detailed description of the data processing method

Nature, context and purpose

DESCRIPTION OF THE NATURE OF THE DATA PROCESSING METHOD
Personal data processing is divided into four sub-processes: 1. Invitation of students to enrol in Example University. 2. Registration of students for enrolment in Example University: A) in person at Example University B) electronic enrolment 3. A professional (clerk) monitors the enrolment process of students and provides assistance in submitting the application form. 4. Execution of registration in Example University . Students can enrol in the Example University by contacting the application point, where they fill in the enrolment form or submit the enrolment electronically. Professionals (clerks) at the Example University monitor enrolment and offer students professional assistance in enrolment if they apply for it.

THE CONTEXT OF PERSONAL DATA PROCESSING
The Example University collects and processes personal data for the purpose of enrolling students in the Example University pursuant to point c. Paragraph 1 of Article 6 of the GDPR, namely: the processing is necessary for the fulfilment of the legal obligation applicable to the controller. The legal basis is Higher Education Act.

WHAT IS THE PURPOSE FOR COLLECTING DATA?
Data are collected for the purpose of enrolment, education and other purposes related to education in the 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 student	Yes	Higher Education Act	Professional staff (clerk)	Permanent
2.	Unique identification number	Yes	Higher Education Act	Professional staff (clerk)	Permanent
3.	Registration number	Yes	Higher Education Act	Professional staff (clerk)	Permanent
4.	Date and place of birth	Yes	Higher Education Act	Professional staff (clerk)	Permanent
5.	State of birth	Yes	Higher Education Act	Professional staff (clerk)	Permanent
6.	Citizenship	Yes	Higher Education Act	Professional staff (clerk)	Permanent
7.	Permanent residence	Yes	Higher Education Act	Professional staff (clerk)	Permanent
8.	Telephone number	Yes	Higher Education Act	Professional staff (clerk)	Permanent
9.	E-mail address	Yes	Higher Education Act	Professional staff (clerk)	Permanent
10.	Grade point average	Yes	Higher Education Act	Professional staff (clerk)	Permanent
11.	Education	Yes	Higher Education Act	Professional staff (clerk)	Permanent
12.	Type of higher education institution	Yes	Higher Education Act	Professional staff (clerk)	Permanent
13.	Type of study program	Yes	Higher Education Act	Professional staff (clerk)	Permanent
14.	Type of direction or module	Yes	Higher Education Act	Professional staff (clerk)	Permanent
15.	Location of study	Yes	Higher Education Act	Professional staff (clerk)	Permanent
16.	Way of study	Yes	Higher Education Act	Professional staff (clerk)	Permanent
17.	Date and academic years of enrolment in the study program	Yes	Higher Education Act	Professional staff (clerk)	Permanent

18.	Year of study	Yes	Higher Education Act	Professional staff (clerk)	Permanent
19.	Number of ECTS credits entered and achieved for each academic year	Yes	Higher Education Act	Professional staff (clerk)	Permanent
20.	Subjects	Yes	Higher Education Act	Professional staff (clerk)	Permanent
21.	Date of application for the examination	Yes	Higher Education Act	Professional staff (clerk)	Permanent
22.	Exam date	Yes	Higher Education Act	Professional staff (clerk)	Permanent
23.	Number of exam repetitions	Yes	Higher Education Act	Professional staff (clerk)	Permanent
24.	Assessment or result achieved during the examination	Yes	Higher Education Act	Professional staff (clerk)	Permanent

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 (c) of paragraph 1 of Article 6 of the GDPR. The legal basis is Higher Education Act.

OTHER METHODS WITH A LOWER LEVEL OF VIOLATION OF THE RIGHT TO PRIVACY
Other methods were not taken into account. The data controller has clearly stated and described the reason, purpose and objective of the data processing. The data processing is carried out in compliance with the legal obligation of the controller.

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 proportional to the purpose of enrolling students in Example University.

IS DATA PROCESSED FOR OTHER PURPOSES?

With regard to the legal basis for the processing of personal data, the Example University has no basis to personal process data outside the purpose, scope or types of processing specified by law.

This does not mean that the Example University is restricted from processing personal data for other purposes if it has an appropriate basis to do so (e.g., individual consent 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

Data, exclusively in anonymised form, are collected and stored in electronic records. Electronic records are accessed only by professional associates (clerks) and the administrator of IT solutions at the Example University with a username and password, who do not have direct contact with students.

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

In order to ensure the adequate protection of personal data and to ensure a uniform approach to data protection within Example University, the Example University will provide training for professionals (clerks) on appropriate conduct regarding data protection, especially regarding the handling of the four-digit password (code).

Professionals (clerk) will sign a "Data Protection Statement".

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 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 student enrolment.

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

		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 law	Professionals (clerk) signed a "Data Protection Statement"	low	medium	low
2	The legal basis is not properly selected	low	high	medium	Through thorough analysis, we found that the basic foundation is the law, which also determines the details of processing	Professionals (clerk) signed a "Data Protection Statement"	low	medium	low
3	Use of legitimate interest by public authorities in the performance of their tasks	medium	high	high	We use a legitimate interest	Professionals (clerk) signed a "Data Protection Statement"	low	medium	low
4	The conditions for consent are not clear	medium	high	high	We do not use consent	Professionals (clerk) signed a “Data Protection Statement”	low	medium	low
5	The terms of consent are not separated by purpose	medium	high	high	We do not use consent	Professionals (clerk) signed a “Data Protection Statement”	low	medium	low
6	An individual is unlawfully coerced into consent in an incompatible relationship with another lawful ground	medium	high	high	We do not use consent	Professionals (clerk) signed a “Data Protection Statement”	low	medium	low
7	Consent is not clearly different from other matters	medium	high	high	We do not use consent	Professionals (clerk) signed a “Data Protection Statement”	low	medium	low
8	Consent is not in clear and simple language	medium	high	high	We do not use consent	Professionals (clerk) signed a “Data Protection Statement”	low	medium	low
9	The consent may not be revoked at any time by an individual	medium	high	high	We do not use consent	Professionals (clerk) signed a “Data Protection Statement”	low	medium	low

10	Consent is not as easy to revoke as to give	medium	high	high	We do not use consent	Professionals (clerk) signed a “Data Protection Statement”	low	medium	low
11	Risks related to the processing of children's personal data	low	high	medium	Children do not participate in the assessment because students are exclusevly adults	Professionals (clerk) signed a “Data Protection Statement”	low	low	low
2	**Legitimate purpose specification and use limitation**			**high**					**medium**
12	The purpose of the processing is not specified	medium	high	high	The purpose of the processing was clearly defined	Professionals (clerk) signed a “Data Protection Statement”	low	medium	low
13	The purpose of the processing is not explicit or clearly defined	medium	high	high	The purpose of processing is clear and it refers to only one purpose of processing	Professionals (clerk) signed a “Data Protection Statement”	low	medium	low
14	The purpose of the processing is not legal	medium	high	high	Through thorough analysis, we confirmed that the purpose of the processing was lawful	Professionals (clerk) signed a “Data Protection Statement”	low	medium	low
15	The retention period is not set	high	high	high	The storage period has been precisely defined	Compliance with storage period	low	medium	low
16	Use of data for another purpose than the purpose for which it was collected	medium	high	high	We guarantee the use of personal data only for a defined purpose	Professionals (clerk) signed a “Data Protection Statement”	low	medium	low
17	Excessive data volume for processing (minimum data volume not used)	medium	high	high	Through thorough analysis, we found that we only process data specified by law	Professionals (clerk) signed a "Data Protection Statement"	low	medium	low
18	Retention period exceeded	medium	high	high	All datas are permanent	Professionals (clerk) signed a “Data Protection Statement”	medium	medium	medium
19	The processing method does not guarantee the security of personal data	medium	high	medium	We control the processing method	Professionals (clerk) signed a "Data Protection Statement"	medium	medium	medium
20	There is no protection against tampering or illegal processing	medium	high	medium	We control the processing method	Professionals (clerk) signed a "Data Protection Statement"	medium	medium	medium
21	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	Professionals (clerk) signed a “Data Protection Statement”	low	medium	low
22	There is no protection against	low	high	medium	We control the processing method, the data are mostly originally in paper form	Professionals (clerk) signed a “Data	low	medium	low

	accidental data corruption					Protection Statement"			
23	Risks related to automated decision making	low	high	medium	We do not make automated decisions	Professionals (clerk) signed a "Data Protection Statement"	low	high	medium
24	Risks related to profiling	low	high	medium	We do not design profiles	Professionals (clerk) signed a "Data Protection Statement"	low	medium	low
3	**Personal information and sensitive information life cycle**			**high**					**medium**
25	Extension of retention period with no legal basis	medium	high	medium	The storage period is permanent (so there is no extension at all)	Professionals (clerk) signed a "Data Protection Statement"	low	medium	low
26	Failure to extend the retention period, where there is a legal basis or at the request of the individual	medium	medium	medium	The storage period is permanent (failure to extend the period cannot even come)	Professionals (clerk) signed a "Data Protection Statement", Upgrade Data Protection Statement	medium	medium	low
27	Undefined procedures of the individual's request after verification if the controller processes data	medium	high	high	We manage risk with pre-prepared form	Pre-pepared form that the individual (student) only fulfill	low	medium	low
28	Undefined procedures of the individual's request for access to data processed by the controller	medium	high	high	We manage risk with pre-prepared form	Pre-pepared form that the individual (student) only fulfill	low	medium	low
29	Undefined procedures for individual's requests after restriction of processing	medium	high	high	We manage risk with pre-prepared forms	Pre-pepared form that the individual (student) only fulfill	low	medium	low
30	Undefined procedures for individual's requests after data deletion	medium	high	high	We manage risk with pre-prepared forms	Pre-pepared form that the individual (student) only fulfill	low	medium	low
31	Undefined procedures of the individual's request for data portability	N/A	high	low	There is no right to data portability due to the processing of data under the law.	Data Protection Policy	N/A	medium	low
32	Undefined procedures in case of an individual's objection	medium	high	high	The process is defined in Data Protection Policy	Upgrade a Data Protection Policy	low	medium	low

33	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	Upgrade a Data Protection Policy	low	medium	low
34	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	Upgrade a Data Protection Policy	low	medium	low
35	Improper implementation of procedures in case of individual's request	high	high	high	The process is defined in Data Protection Policy	Upgrade a Data Protection Policy	low	medium	low
36	Improper implementation of procedures in case of an individual's request for deletion of data	high	high	high	The process is defined in Data Protection Policy	Upgrade a Data Protection Policy	low	medium	low
37	Improper implementation of procedures in case of an individual's request for data portability	N/A	high	low	There is no right to data portability due to the processing of data under the law.	Data Protection Policy	N/A	medium	low
38	Improper implementation of procedures in case of the objection of an individual	high	high	high	The process is defined in Data Protection Policy	Upgrade a Data Protection Policy	low	medium	low
39	Unnecessary processing of special categories of personal data	low	high	medium	We do not process special categories of personal data	Upgrade a Data Protection Policy	low	high	low
40	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		Concluding a contract for processing and control, Design of good practices	medium	medium	medium
41	No data protection impact assessment has been produced	low	high	medium		Implementation of the DPIA	low	medium	low
4	**Accuracy and quality**			**high**					**medium**
42	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	medium	low
43	An individual's data is not updated when the individual changes it	medium	high	high	The procedure for data processing is defined in the data protection policy	Upgrade a data protection policy	low	medium	low

44	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	Upgrade a data protection policy	medium	medium	low
45	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-pepared form that the individual (student) fills out	low	medium	low
46	Improper implementation of procedures when requesting an individual to correct data processed by the controller	low	high	medium	The procedure for data processing is defined in the data protection policy	Upgrade a data protection policy	low	medium	low
5	**Openness, transparency and notice**			**high**					**medium**
47	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
48	Information presented to the individual is not uniform for all controllers and processors	high	high	high	It is evident from the existing privacy statements that the information is uniform	Data protection policy	medium	medium	medium
49	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 comprehensive instructions are not provided	Upgrade a data protection policy	medium	medium	medium
50	Information is not provided to an individual when obtaining personal information	high	high	high	The enrolment form does not include an attachment with a privacy statement	Suplement the enrolment form with a privacy statement	low	medium	low
51	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	medium	low
6	**Individual participation**			**high**					**low**
52	The portable data received by an individual are not machine-readable	N/A	high	low	There is no right to data portability due to the processing of data under the law.		N/A	medium	low
53	The portable data received by an individual is incomplete	N/A	high	low	There is no right to data portability due to the processing of data under the law.		N/A	medium	low
54	The decision made by automatic	medium	high	high	We do not use automated decision making		low	medium	low

	decision-making is final							
55	Automatic listing of an individual is definitive	medium	high	high	We do not use profiling		low	medium	low
56	For the joint controllers, the agreement does not clearly set out all the rights and obligations of each of the controllers	N/A	high	low	We are not joint controllers		N/A	high	low
57	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
58	There is no designated contact point for the individual	medium	high	high	We designated contact point for the individual	Publicly published contact data (on the website)	low	medium	low
59	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
60	There is no designated data protection authority	medium	high	high	We have named a DPO	Concluding a contract for processing and control	low	medium	low
61	The contact details of the Data Protection Officer are not accessible to the individual	medium	high	high	We have published the DPO's contact information	Concluding a contract for processing and control	low	medium	low
7 Accountability				**high**					**low**
62	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	Concluding a contract for processing and control	low	medium	low
63	The tasks and responsibilities of the Data Protection Officer are not clearly defined	medium	high	high	We have defined the DPO's tasks and responsibilities	Concluding a contract for processing and control	low	medium	low
64	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.	Concluding a contract for processing and control	low	medium	low
8 Security safeguards				**high**					**low**

65	There are no documented security policies for protecting personal information	medium	high	high	We have our own security policies and risk assessment	Upgrade a data protection policy	Low	Medium	low
66	There is no documented processing of personal data 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
67	Organisational measures for the protection of personal data are not clearly defined	medium	high	high	We have our own security policies and risk assessment	Upgrade a data protection policy	low	medium	low
68	There are no clearly defined technical measures for the protection of personal data	medium	high	high	We have our own security policies and risk assessment	Upgrade a data protection policy	low	medium	low
69	Organisational measures to protect personal data are not sufficient	medium	high	high	We have our own security policies and risk assessment	Upgrade a data protection policy	low	medium	low
70	Technical measures to protect personal data are not sufficient	medium	high	high	We have security policies and high technical standards	Upgrade a data protection policy	low	medium	low
71	Organisational measures to protect personal data are not being implemented	medium	high	high	We have our own security policies and risk assessment	Upgrade a data protection policy	low	medium	low
72	No technical measures are in place to protect personal data	medium	high	high	We have our own security policies and risk assessment	Upgrade a data protection policy	low	medium	low
73	There is no regular check on security controls	medium	high	high	We have our own security policies and verification procedures	Upgrade a data protection policy	low	medium	low
74	Organisational controls for the protection of personal data are not clearly defined in contracts with processors	high	high	high	We do not have a data processing contract		N/A	medium	low
75	Technical control contracts for the protection of personal data are not clearly defined in contracts with processors	high	high	high	We do not have a data processing contract		N/A	medium	low

9	**Monitoring, measuring, reporting**			**high**					**medium**
76	The Data Protection Officer does not guarantee the implementation of privacy impact assessments	medium	high	high	We perform impact assessments	Concluding annual tasks plan for the DPO	low	medium	low
77	The Data Protection Officer does not check compliance with the regulations	medium	high	high	We perform compliance checks, also with DPIA	Concluding annual tasks plan for the DPO	low	medium	low
78	The Data Protection Officer does not educate employees	medium	high	high	We educate, train and inform our employees	Concluding annual tasks plan for the DPO	low	medium	low
79	The Data Protection Officer does not cooperate with the supervisory authority	medium	high	high	The DPO cooperates with the supervisory authority (DPO sends requests for an opinion or, in the ex-ante advisory procedure, forwards the impact assessment)	Concluding annual tasks plan for the DPO	low	medium	low
80	No reporting regarding the correction of personal data is introduced	high	high	high	Data is known for claims submitted to Example University	Data protection privacy	medium	medium	low
81	No reporting regarding the deletion of personal data is introduced	medium	high	high	Data is known for claims submitted to Example University	Data protection privacy	medium	medium	low
82	There is no documented content reporting on an individual's personal information	medium	high	high	Data is known for claims submitted to Example University	Data protection privacy	low	medium	low
83	Reporting on the transfer of individual data to third parties is not introduced	high	high	high	We are only controller		low	medium	low
84	Copies of personal data provided as part of the right to data portability have been preserved longer than the retention period	N/A	high	low	There is no right to data portability due to the processing of data under the law.		N/A	medium	low
85	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 processing of new personal data.		low	medium	low
86	There are no policies in place to design and maintain records	medium	high	high	We carry out our activities in accordance with the instructions of our DPO	Concluding annual tasks plan for the DPO	medium	medium	medium

	of processing activities							
87	Recipients of personal data are not identified	medium	high	high	Example University is the only recipient of personal data	Data protection policy	low	medium	low
10	**Preventing harm**			**high**					**medium**
88	Guidelines for determining the legality of processing have not been established	medium	high	high	We use EDPB's guidelines and infographics as well as those from the information commissioner	Data protection policy	low	medium	low
89	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	Upgrade a data protection policy	medium	medium	medium
90	There is no adequate safeguard for decision making based on special categories of personal data	medium	high	high	We do not process special categories of personal data	Upgrade a data protection policy	low	medium	low
91	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.	Upgrade a data protection policy	medium	medium	medium
92	No rules and procedures have been put in place to minimise the harm to an individual when archiving in the public interest	medium	high	high	When storing information, we keep only the data specified by law	Upgrade a data protection policy	Low	medium	low
93	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 research purposes	low	high	medium	For scientific research purposes, we only use anonymised data	Upgrade a data protection policy	low	medium	low
94	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	low	low	low
11	**Supplier / third party management**			**high**					**medium**

95	No outsourcing management policies are in place	low	high	medium	We do not have outsourcing	Data protection policy	low	low	low
96	Outsourcing arrangements do not contain sufficient guarantees that adequate organisational measures are in place to protect personal data	high	high	high	We do not have outsourcing	Data protection policy	medium	medium	medium
97	Outsourcing arrangements contain sufficient guarantees that adequate technical measures are in place to protect personal data	high	high	high	We do not have outsourcing	Data protection policy	medium	medium	medium
98	Sufficient restrictions and rules for hiring sub-contractors have not been applied	high	high	high	We do not have outsourcing	Data protection policy	medium	medium	medium
99	Procedures and duration of processing are not specified in the agreement with the processors	high	high	high	We do not have outsourcing	Data protection policy	low	low	low
100	The purpose and type of processing is not specified in the agreement with the processors	high	high	high	We do not have outsourcing	Data protection policy	low	low	low
101	The types of personal data subject to processing are not specified in the agreement with the processors	high	high	high	We do not have outsourcing	Data protection policy	low	low	low
102	The types of individuals whose personal data are subject to processing are not specified in the agreement with the processors	high	high	high	We do not have outsourcing	Data protection policy	low	low	low
103	In agreement with the processor, not all 8 obligations are specified as per Article 28 paragraph 3 of the GDPR	high	high	high	We do not have outsourcing	Data protection policy	low	low	low

104	The agreement with the processor does not specify the obligation and the procedure for reporting incidents	high	high	high	We do not have outsourcing	Data protection policy	medium	medium	low
105	There are no requirements for the processor to outsource his work	high	high	high	We do not have outsourcing	Data protection policy	medium	medium	low
106	There are no procedures in place to ensure that processors comply with the requirements of the controller	high	high	high	We do not have outsourcing	Data protection policy	low	medium	low
107	There are no procedures in place for the employee of the controller to comply with the requirements of the controller	high	high	high	Compliance with the requirements of the controller is in the description of the employee's work tasks.	Employment contract	low	medium	low
12	**Breach management**			**high**					**low**
108	Procedures for notifying the supervisory authority of incidents have not been established	medium	high	high	The DPO notifies the supervisory authority with the consent of the Example University dean	Concluding annual tasks plan for the DPO	low	medium	low
109	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 dean	Concluding annual tasks plan for the DPO	low	medium	low
110	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**
111	Privacy and security policies do not respect the rights of the individuals	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
112	Privacy and security policies do not respect the freedoms of the individuals	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
113	Privacy and security policies do not take into account the legitimate interests of the individuals	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

114	Automatic procedures do not involve 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
115	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
116	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	medium	medium	medium
117	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**
118	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
119	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
120	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
121	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.

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 processor is suitable and appropriate.

RISK GROUP	THE HIGHEST RISK BEFORE MEASURES	THE HIGHEST RISK AFTER MEASURES
1 Choice and consent	high	medium
2 Determination of lawful purpose and limitation of use	high	medium
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
According to the result of the privacy impact analysis, an approach in which the Example University is the controller and processor is appropriate, as in case of implementing measures not pose a major risk to the rights and freedoms of the data subjects. A key prerequisite for the proper regulation of contractual relations is the existence of a written contract on data processing (this can also be concluded in an equivalent electronic form). Example University must have concrete procedures and measures to protect personal data (must be visible whose data and for what purpose the data will be processed). Only references to GDPR requirements or provisions such as "data will be protected under the GDPR" are not sufficient. Procedures and measures for data security need to be defined and concretised (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, provided, of course, that these rules are appropriate. For this purpose, the University also uses privacy statements, which clearly state how personal data is protected (both from a technical point of view and from an organisational point of view).

Self-assessment

In order to self-assess the compliance of the prepared DPIA with the regulations and guidelines of the Information Commissioner, we performed a self-assessment of the prepared impact assessment according to the criteria for assessing the adequacy of DPIA and in accordance with the Guidelines on Data Protection Officers of Article 29 16 / EN WP 243 rev. 01.

Requirement	Reference	Self-assessment
A systematic description of the processing is given (Article 35 (7a))		
The nature, scope, context and purposes of the processing are taken into account (recital 90)	The main explanation is in the subsection »Description of the nature of the data processing method.	The assessment addresses the requirement from the guidelines
The data set, operators and users, and storage periods are defined	The set of data is defined in the subsection: »Personal data processing«. The controller is defined in the subsection: »Risk assessment for the rights and freedoms of data subjects, where the Example University is the controller«	The assessment addresses the requirement from the guidelines
A description of data flows and involved entities is given	Data flows and involved entities are described in the subsection »Description of the nature of the data processing method« and »What is the purpose for collecting data? «	The assessment addresses the requirement from the guidelines
A description of the means of processing (hardware and software, networks, human resources and the means of communication used) is given.	The description of the means of processing is given to the level that is possible according to the available data and is described in the subsection »The context of personal data processing«	The assessment addresses the requirement in the guidelines to the level of limitation of this analysis
Compliance with approved codes of conduct is taken into account (Article 35 (8))	Codes of conduct have not yet been adopted	The assessment addresses the requirement from the guidelines
An assessment of necessity and proportionality is given (Article 35 (7b)) and measures are identified to ensure coherence, including measures that contribute to pursuance of necessity and proportionality and adherence to fundamental principles		
Specific, explicit and legitimate purpose(s) (Article 5 (1b))	The purpose of processing is discussed in the subsection »What is the purpose for collecting data? «	The assessment addresses the requirement from the guidelines
Lawfulness of processing (Article 6)	The lawfulness of processing is set out in the subsections: »The context of personal data processing« and »Legal basis for data processing«	The assessment addresses the requirement from the guidelines

The processing is adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed (Article 5(1c))	The adequacy and relevance for each process is discussed separately in the subsections: »Risk assessment methodology for the rights and freedoms of data subjects« with the support of the matrix for assessing the adequacy, proportionality and relevance of personal data.	The assessment addresses the requirement from the guidelines
Storage limitation is taken into account – storage periods (Article 5(1e))	Limitations of storage periods are analysed in the matrices for assessing the adequacy, proportionality and relevance of personal data in the subsection "Personal data processing".	The assessment addresses the requirement from the guidelines
An assessment of necessity and proportionality is given (Article 35 (7b)) and measures are identified to ensure compliance, which include measures that contribute to the protection of the rights of the data subjects.		
Informing the data subject about data processing (Articles 12, 13 and 14)	Included in the risk assessment »Risk assessment for the rights and freedoms of data subjects, where the Example University is the controller«	The assessment addresses the requirement from the guidelines
Right of access and data portability (Articles 15 and 20)	Included in the risk assessment »Risk assessment for the rights and freedoms of data subjects, where the Example University is the controller«	The assessment addresses the requirement from the guidelines
Right to rectification and erasure of data (Articles 16, 17 and 19)	Included in the risk assessment »Risk assessment for the rights and freedoms of data subjects, where the Example University is the controller«	The assessment addresses the requirement from the guidelines
Right to object and right to restriction of processing (Articles 18, 19 and 21)	Included in the risk assessment »Risk assessment for the rights and freedoms of data subjects, where the Example University is the controller«	The assessment addresses the requirement from the guidelines
Relations with (contractual) processors (Article 28)	Not applicable, because Example University is the only controller and processor.	The assessment addresses the requirement from the guidelines
Safeguards regarding transfers of data to third countries (Chapter V.)	Discussed in subsection »TRANSFER OF DATA TO THIRD COUNTRIES« and included in the risk assessment: »Risk assessment for the rights and freedoms of data subjects, where the Example University is the controller«	The assessment addresses the requirement from the guidelines
Prior consultation (Article 36)	The analysis concludes that the controller to whom the regulations apply does not have a direct influence on the regulation, but that the prior consultation should be carried out by the legislator or the proposer of the law.	The assessment addresses the requirement from the guidelines
Risks to the rights and freedoms of the data subjects are managed by assessing the origin, nature, specificity and severity of the risks (recital 84), with the risks being assessed from the point of view of the data subject by		

The sources of risk were taken into account (Recital 90)	The sources of risks were determined by a predefined systematic methodology, described in the subsection »Risk assessment methodology for the rights and freedoms of data subjects«	The assessment addresses the requirement from the guidelines
Possible effects on the rights of the data subject in the event of illegal access, alteration or loss of data are taken into account	The effects on the rights of the individual have been taken into account by a pre-defined systematic methodology described in subsection »Risk assessment methodology for the rights and freedoms of data subjects«	The assessment addresses the requirement from the guidelines
The likelihood and severity of the risk were assessed (Recital 90)	The likelihood and severity of the risks are assessed in the subsection »Risk assessment for the rights and freedoms of data subjects, where the Example University is the controller«	The assessment addresses the requirement from the guidelines
The risks for the rights and freedoms of the data subject are addressed		
The measures for addressing the risks are defined (Article 35(7d) and Recital 90)	Risk management measures according to the level of detail of the analysis and limitations of the analysis are defined in the subsection »Risk assessment for the rights and freedoms of data subjects, where the Example University is the controller«	The assessment addresses the requirement from the guidelines
Stakeholders are involved		
Where appropriate, views of data subjects or their representatives have been obtained (Article 35(9))	The analysis concludes that the controller to whom the regulations apply does not have a direct influence on the regulation, but that the prior consultation should be carried out by the legislator or the proposer of the law.	The assessment addresses the requirement from the guidelines