International Journal of Management, Knowledge and Learning, 8(2), 221–241

Data Privacy Assessment: An Exemplary Case for Higher Education Institutions

Ali Habbabeh
University of Applied Sciences and Arts Northwestern Switzerland

Bettina Schneider
University of Applied Sciences and Arts Northwestern Switzerland

Petra Maria Asprion
University of Applied Sciences and Arts Northwestern Switzerland

The European General Data Protection Regulation (GDPR), which became applicable in May 2018, obliges companies and thus Higher Education Institutions (HEIs) to (re)assess their data privacy procedures, in particular the processing of personal data. As the new law unfolds an extraterritorial scope, HEIs located outside the European Union (EU) also need to examine whether they are affected, and, if so, take the necessary measures. There is a lack of discussion and approaches in the current literature as to how HEIs can comply with the GDPR regulations. The aim of this study is therefore to analyse scientific publications in order to deliver two results: Firstly, consolidated relevant recommendations and requirements in the context of GDPR, and, secondly, an instrument to help HEIs to raise their GDPR awareness. The latter was built by applying design science guidelines and resulted on a whole of 44 controls that yield a total score. The resulting value can serve as an indicator of HEI's accordance with GDPR regulations. In addition, the compiled controls can be used as a management instrument to assess the measures taken and to continuously promote compliance with GDPR.

Keywords: assessment instrument, assessment tool, data privacy, European General Data Protection Regulation, higher education institutions

Introduction

The right to privacy in Europe is considered fundamental, as stated in Article 8 of the European Convention on Human Rights (European Court of Human Rights, 2018): 'Everyone has the right to respect for his private and family life, his home and his correspondence.'

The headlines of the recent news highlight the serious consequences faced by some companies after abuse of privacy was made public. One of the best-known case occurred in 2018, when Cambridge Analytica, a British political data analysis company, announced that they had mistakenly ac-

quired data from tens of millions Facebook users without their consent and then used these data to try to influence political decision-making, namely the US presidential election (Wong, 2019). The data breach led to a loss of reputation along with a financial one represented by a drop in Facebook's stock price of 17.44 points (Segarra, 2018). To minimize occurrence of such incidents, the European Union (EU), on 27th of April 2016, approved the General Data Protection Regulation (GDPR), a law that unfolds extraterritorial scope and therefore affects organizations worldwide (The European Parliament and The Council of the EU, 2016). This newly created regulation has obliged all EU Member States to integrate the legal provisions into their own national law by 6 May 2018 (Albrecht, 2016).

Like other organizations, Higher Education Institutions (HEIs) rely heavily on the processing of personal data and are concerned with GDPR in case they reside in the Union or process data from people who are in the EU. This study focuses on HEIs in Switzerland – not part of the EU; yet these organizations are likely to process data of individuals residing in the EU, such as students, alumni or parents of students or alumni. Even though Switzerland has a long tradition in data privacy and is a highly internationalized country, more emphasis needs to be placed on the EU regulation. A recent survey by the Swiss ZHAW School of Management and Law reports that, although the majority of Swiss companies surveyed consider data protection as important or rather important, the GDPR is not sufficiently well known. In addition, only about a quarter of the companies expect to be affected by the EU regulation (Ebert & Widmer, 2018). This is contrary to the estimates of various stakeholders (e.g., lawyers, consultants), who assume that the majority of Swiss companies are concerned (Lurati, 2018; Müller, 2017). Turning to the specific case of HEIs in Switzerland, there has been a lack of specific studies regarding GDPR, thus this study aims to contribute to close the gap. As the Swiss data protection law is currently under review and is expected to converge on EU standards, some guidance for Swiss HEIs to support GDPR compliance will be a useful contribution to academia and practice. Additionally, since this study focuses on Switzerland as a non-EU country, the results of this research can also be applied to other non-EU countries.

The purpose of this work is to emphasize the importance of data privacy compliance for HEIs and to provide a prototypical assessment instrument for HEIs in Switzerland that could be utilized to analyse the institutions' readiness to follow GDPR. The assessment instrument allows the measurement of performance on GDPR, with tailored questions that are understandable to compliance specialists who can test the prototype and use it as a first and quick auditing tool.

We have worked out two research questions: (1) What are the GDPR's re-

Table 1 Literature Search Parameters Applied for This Research

Parameter	Value
Language of Publication	English
Subject Area	Legal, Business
Business Sector	Education, other (Data privacy/GDPR related)
Geographical Area	EU, Switzerland
Publication Period	Last 5 years, plus exceptions for classical publications
Literature Type	Books, scientific papers, refereed journals, practitioner papers

quirements for HEIs? This first question is relevant because our study sets a specific focus on Switzerland and the organizational type of HEIs as an exemplary unit of analysis. Even though GDPR is a regulation that applies to all industries, each sector is facing its particular challenges due to different types of data to be processed. (2) How could a GDPR assessment instrument look like to support Swiss HEIs' compliance with the law? This second question is relevant, as our study not only aims to investigate challenges, but also to achieve practical benefits. As the survey of ZHAW School of Management and Law (Ebert & Widmer, 2018) shows, Swiss companies – this includes HEIs – should be more concerned to comply with GDPR. Therefore, providing them with a well-adopted assessment instrument, could serve as a means to raise awareness.

To answer the research questions, the first methodological step was a literature review according to the guidelines of Saunders, Lewis, and Thornhill (2009). The chosen procedure relies on the definition of search parameters for obtaining relevant literature. As to the scope of this study, the selected parameter values are listed in Table 1.

As a second methodological approach, the Design Science Research (DSR) guidelines of Hevner & Chatterjee (2010) were applied. According to Hevner, Salvatore, Jinsoo, and Sudha (2004), DSR must lead to an artefact, which could be a construct, model, method or an instantiation and it aims to align technical and business aspects. This was considered suitable for our research, which aims to yield a GDRP assessment tool. A first version of the tool was derived using information gained from the existing knowledge base and from the HEIs' environment in Switzerland. The prototype was then improved on the basis of an evaluation obtained by a team of experts in the fields of governance, risk and compliance. In the future, a continuous improvement cycle should further sharpen the performance of the assessment instrument.

To develop the intended tool, the DSR approach is well-suited to align research processes with real-world problems and to integrate business with technical aspects. Figure 1 shows how the research framework of Hevner et

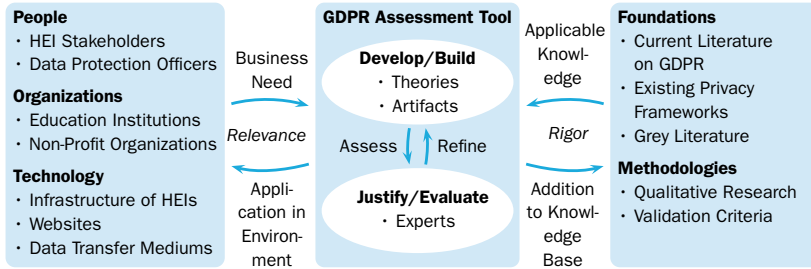


Figure 1 Research Framework of This Study (Adapted from Hevner et al., 2004)

al. (2004) was adapted. The knowledge base, represented with the systematic literature review, allowed to build and evaluate the intended 'GDPR Assessment Tool for HEIs' and constituted the rigor cycle. On the other hand, the environment, represented by HEIs in Switzerland and its surrounding, composed the relevance cycle, which the artefact drew its relevance from.

The remainder of our paper is structured as follows. First some backgrounds about GDPR are described, followed by an elaboration of requirements the GDPR places on the universities. Afterwards, an analysis of the selected existing assessment instruments follows and promotes the development and evaluation of our HEI-specific GDPR assessment tool. Finally, conclusions are drawn and an outlook on future research is given.

GDPR Background

As stated by Albrecht (2016), GDPR will not only change Europe, but the world. The intention behind the GDPR is related to the protection of natural persons (individuals) with regard to the processing of their personal data. To achieve this objective, in 2018 the new regulation became enforcable to catch up the threats of cyber-attacks and to respond to those threats and ensure future resilience (Krystlik, 2017).

One of the changes compared to the GDPR's predecessor Data Protection Directive 95/46/EC is the extended territorial scope (Tikkinen-Piri, Rohunen, & Markkula, 2018). According to Article 3, GDPR is obligatory for organizations established in the EU, but also applies to organizations located outside of the EU if they offer goods or services to EU residents or monitor the behaviour of individuals in the EU (Tikkinen-Piri et al., 2018). In simplified terms, GDPR governs any organization that processes personal data of EU individuals – referred to as 'data subjects.' Based on this, HEIs outside the EU, e.g. in Switzerland, may also be subject to the GDPR if they handle data of persons such as students living in an EU member state.

Any organization affected by GDPR, needs to adhere to the following key principles (ICO, n.d.; Tikkinen-Piri et al., 2018): data processing must hap-

pen in a lawful, transparent, fair manner that ensures appropriate security and data collection has to be reduced to the minimum necessary in relation to the processing purpose. In addition, personal data shall be accurate and kept in a form that permits identification of individuals no longer than required. Finally, the accountability principle requires organizations to take responsibility and demonstrate compliance.

In addition to these principles, noteworthy developments with regard to consent lead to the necessity, amongst other things, for consent to be given freely and to reflect a specific, informed and explicit indication of the wishes of the data subject (Tikkinen-Piri et al., 2018).

According to the Information Commissioner's Office (ICO), the UK's supervisory authority, the obligations under the GDPR vary depending on the role an organization is assuming. A HEI would usually be considered as a 'data controller,' referring to a person or an agency that decides on the goals of personal data processing. Being a data controller comes with a high level of compliance responsibility – not only for oneself but also for potential processor(s), persons or agencies that carry out data processing on behalf of a controller (ICO, n.d.).

GDPR expands the data subject's rights. This includes the right to access information held on the data subject and the right to object to the processing of personal data where there are legitimate grounds for doing so (Tankard, 2016). As a further example, the right to be forgotten requires data controllers and processors to remove data that is no longer relevant or is considered to be inadequate or irrelevant (Tankard, 2016). Besides the data subject rights (for which a full list will be provided in section 4 of this paper), GDPR imposes enhanced obligations on data processors and controllers. As an example, appropriate technical and organizational measures to ensure data protection, such as encryption, are required (Tikkinen-Piri et al., 2018). In Article 25, GDPR sets out the concept of 'data protection by design and default' and Article 30 describes the obligation to maintain records of processing activities (Tikkinen-Piri et al., 2018). The obligations will be covered in more detail throughout this study.

A lot of attention in media has focused on the sanctions for not complying with GDPR (Garber, 2018). According to Article 84, companies can be fined up to 20 million euros or 4% of the total worldwide annual turnover, whichever is higher (Tankard, 2016). Hence, any Swiss HEI affected by GDPR should be concerned with the conformity to the law. Beyond the avoidance of fines, GDPR can also be seen as an opportunity to improve data processing practices and safeguards that strengthen stakeholder confidence and avoid business disruption (Garber, 2018).

The Data Protection Commission, the national independent data protection authority in Ireland, divides the GDPR into specific areas that need to

be tackled during implementation (Data Protection Commission, 2017, p. 8). These seven areas are:

- Personal Data Collection
- Data Subject Rights
- Accuracy and Retention
- Transparency Requirements
- Data Controller Obligations
- Data Security
- Data Transfer (if applicable)

This study uses these seven areas as high-level topics when setting up the prototype of a GDPR assessment instrument and they will be discussed in detail in the following sections.

Existing GDPR Approaches and Assessment Instruments

After an introduction to GDPR, this chapter focuses on the specific requirements that the law places on HEIs. To achieve this, three alternative approaches towards GDPR compliance dedicated to the needs of HEIs are presented, one by Microsoft (2018), another by Podnar (2017) aimed at American HEIs, and the last one by the UK author Cormack (2017). In addition, some existing GDPR assessment instruments will be introduced – not focused on dedicated industry needs – that serve as a source for the development of the prototype.

Recommendations towards GDPR Compliance for HEIs

Microsoft released a guide for educational institutions on GDPR. In this guide, the authors defined two bodies of data in HEIs: the curriculum and the organization's information collection about employees and students (Microsoft, 2018). The Microsoft guide offers a variety of challenges and recommendations that revolves around four key steps:

1. *Discover:* a HEI must identify what personal data it holds and where. One challenge here is to document the way the data is processed in a GDPR-compliant method. Another issue is keeping track and checking the bandwidth of the devices on which data is stored, something that can be difficult if a non-managed cloud is included.
2. *Manage:* personal data must be governed. It is vital to identify the reason behind each data collection and question if it is necessary for the education delivery process in each HEI. The challenge here is to meet the strict GDPR rules on securing data across multiple data sources that a HEI uses – such as USB sticks, paper files in

cabinets, and others. Moreover, HEIs must be transparent on which personal data they collect when new students register and identify if this data is needed to fulfill their missions.

3. *Protect:* a HEI must have security standards in place to detect and prevent data breaches. This includes encrypting emails, adding rights to individual files and, most importantly, educating students and staff on cybersecurity and best practices when they use external devices to access their HEI's data. It is essential to remember that GDPR is an ongoing journey and not a destination. Therefore, a HEI should also conduct regular testing and constantly evaluate the effectiveness of their cybersecurity measures.
4. *Report:* as required by GDPR, a HEI must have the suitable documentations, respond to data access requests and report data breaches if they occur. GDPR hands over the responsibility of safeguarding personal data to the organization. Thus, a HEI must demonstrate its compliance with GDPR requirements. A HEI should facilitate data protection impact assessments (DPIAs), maintain audit trails, and track the flow of data to third parties when conducting audit trails. Moreover, a HEI should be able and have the necessary tools to respond to data breaches and report them within 72 hours to the authorities as required by GDPR (Microsoft, 2018).

Podnar (2017), a digital governance adviser, suggests an alternative approach for the GDPR compliance journey adapted to HEIs. The recommendations begin by conducting an audit on the HEIs' data. HEIs must document the location of data storage, the type of data collected, who has access to that data, and the reason for its collection. Some examples of the type of data HEIs typically collect, which need to be considered for the audit process, are (Podnar, 2017):

- Academic records,
- Alumni donations records,
- Students' pictures and other information used in students' IDs, even health data,
- Records of the use of websites and other tools offered by HEIs to students and researchers.

The second step deals with the lawfulness of data processing, whereas it is especially relevant to recognize the touchpoints where a consent, as one of the six possible lawful bases, is required (The European Parliment and The Council, 2016, Art. 6). The approach suggests a mapping of all the personal data that a HEI collects to determine the points at which consent should be collected. The third step of Podnar's approach is to develop

'a GDPR-compliant copy' of the consent and the required notifications including, among other things, the reasons for data collection along with the duration of the processing. Moreover, the data subjects must be informed of their rights to remove or access to their data (The European Parliment and The Council, 2016, Art. 30). Next, Podnar recommends HEIs to develop a communication plan. This is related to Article 33 of the law obliging data controllers to report personal data breaches that are likely to result in a risk to the rights and freedoms of individuals to the supervisory authority within 72 hours after detection.

As a final step, a HEI needs to decide if a Data Protection Officer (DPO) is required or not. Though the approach does not specify how to determine whether a HEI needs a DPO, according to Article 37, a DPO is obligatory for public bodies. Therefore, if a HEI is public, then a DPO is mandatory. However, it is relevant to recognize Article 27, which refers to data controllers who are not established in the EU, as in the case of Swiss HEIs. According to this Article, a so-called 'representative' has to be designated, whereas the obligation does not apply to public authorities or bodies (The European Parliment and The Council, 2016, Art. 27).

Turning to the recommendations of another author, Cormack (2017) regards the increased accountability regarding data held by HEIs as a significant change to GDPR. The author advocates that HEIs must have adequate measures in place to ensure the security of the information about students and employees.

In total, there are seven steps that HEIs must take to become ready for GDPR:

1. *Prepare:* Cormack (2017) suggested that the first step is to spread awareness of GDPR throughout the HEI. The GDPR assessment instrument being developed as a result of this study would be an instrument to support this preparatory phase of awareness building.
2. *Be in the know:* The HEI must document and be informed of the data it holds, and the source of that data, and have a plan in the event of a data breach. This step concerns the principle of accountability.
3. *Assign a DPO:* An internal or external employee who has the appropriate knowledge to ensure compliance with GDPR should be assigned as a DPO. As Cormack is targeting HEIs in the UK, this would be mandatory; however, exceptions could possibly apply to non-EU controllers (see our remark related to the data protection representative).
4. *Review privacy notes:* HEIs must reconsider their privacy agreements and make sure that the process of collecting personal information from students and employees is legal, time limited, and compliant with the required GDPR rules. This step is connected to the lawfulness

of data processing. Some processing activities might be covered by a contract or public, legitimate and vital interest. However, in case such a legal base is missing, data subjects must be asked for consent.

5. *Ensure that an individual's rights can be upheld:* Data subjects, be it students, parents or employees, have many rights under the GDPR, such as: have faulty information corrected, forbid direct marketing, have their data deleted, and move their data to another institution (data portability).
6. *Review how consent is given:* A HEI must ensure that the way it collects consents from its data subjects is in accordance with GDPR. For example, consents must be freely given, specified for only one processing, and cannot be implied by inactivity, such as a pre-checked box in an online form.
7. *Data breach drills:* Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, HEIs must inform the supervisory authority within 72 hours after having become aware of the event (The European Parliment and The Council, 2016, Art. 33).

This study takes into account the three approaches presented in setting up the GDPR assessment instrument for HEIs in Switzerland.

Existing GDPR Assessment Instruments

There exist already several GDPR assessment instruments for organizations, such as the ICO's data protection self-assessment (ICO, n.d.), the online 'quick-check' from the Swiss organization Economiesuisse (n.d.) or the self-assessment of the German (Bavarian) authority for data protection (BayLDA, n.d.). Those instruments are focused on a specific target group and of limited relevance for HEIs. In the following, we introduce two instruments, which we selected and used as a foundational source for the intended GDPR assessment instrument; we selected both because of their high maturity.

ISACA Assessment Instrument

The first instrument investigated more deeply is the 'ISACA-CMMI GDPR Assessment.' It was chosen because ISACA is a very well-established organization with huge expertise in the field – among others – of data privacy, governance and compliance. The instrument 'provides users with a roadmap for GDPR implementation based on the answers to a series of questions/statements' (ISACA, n.d.). ISACA's solution consists of privacy-related questions, each one mapped to the corresponding GDPR law articles. As an example, there is a statement focusing on the obligation to

maintain a register of data processing activities (The European Parliment and The Council, 2016, Art. 30): 'Personal data is documented in terms of their metadata in a register that is auditable and complete. The register provides a definitive record of what is processed and why.' (ISACA, 2018). Additionally, a reference to various principles from ISACA's well-established IT control frameworks is given (e.g., COBIT5 framework for strategic enterprise governance of IT).

Each question of ISACA's GDPR assessment can be answered in four different ways according to 'fully achieved,' 'largely achieved,' 'partially achieved' or 'not achieved.' Besides these options, it is possible to skip questions or to mark them as not applicable (ISACA, 2018). After the online questionnaire is completed, a comprehensive summary report will be compiled with the possibility to download. The evaluation divides the various GDPR-questions into categories and indicates the resulting state using text along with amplification. The text contains advice as to what needs to be done to comply with the law.

Even though ISACA's solution is comprehensive, the instrument might not be easy to use by non-specialists in the organization, due to its lengthy legally-based questions. Each question of ISACA's instrument belongs to one or more GDPR articles and can contain up to eight articles in the same question.

Irish Data Protection Commission Checklist

The checklist from the Irish GDPR supervisory authority was chosen because of the compact nature of the instrument, and the similarity to ISACA, yet in a more easy-to-use form. It is a questionnaire-based guide divided into several sections, grouping GDPR-related questions. In contrast to the ISACA instrument, the Data Protection Commission questions have to be answered with either 'yes' or 'no' (Data Protection Commission, 2017). Moreover, the questions in the Data Protection Commission checklist are shorter and each belongs to one or two articles of the GDPR. An extra column is provided in the instrument for comments or remedial actions. However, the Data Protection Commission solution did not address some details such as third-party management. Still, the instrument has overlaps with the ISACA solution and includes similar questions.

Development of a GDPR Assessment Instrument for HEIs

In this chapter, we will present the steps of the development of our prototypical GDPR assessment instrument for Swiss HEIs. Based on selective concepts, existing recommendations and instruments presented, three stages were identified for a complete GDPR assessment.

1. *Check GDPR applicability:* In this stage, a HEI should first ensure whether it is under the scope of the GDPR. This stage's outcome must be a simple 'yes' or 'no.'
2. *Assess GDPR readiness:* In this stage, a DPO, or if not existent, a similar function, should answer questions associated with GDPR in order to get a result that indicates the HEI's readiness level to comply with the law.
3. *Act towards GDPR compliance:* In this stage, a HEI should act upon the result of the previous assessment. This stage is not in the scope of the current study.

The prototype developed adapts parts of the existing GDPR assessment instruments and combines them into an instrument for HEIs residing outside EU – Switzerland was chosen as a concrete unit of analysis. Due to their compactness and simplicity, the general outlines of the Data Protection Commission checklist were adopted. However, many of the ISACA instrument's controls have been used to fill any gaps the Data Protection Commission instrument missed. To tailor the instrument to HEI's needs, the majority of questions required an adjustment. Process models of each stage were created as a new element, using Business Process Model and Notation (BPMN) 2.0. They are designed to help users go through the assessment in the intended order (Figure 2).

Stage 1: Check GDPR Applicability

The first stage of this assessment instrument is to identify whether GDPR applies to a specific HEI or not. In his publication, Varankevich (2017), a data privacy officer and GDPR consultant, introduced a flow chart that can be used to determine the applicability of GDPR to any organization. If the outcome of this part is 'GDPR does not apply' then the rest of the assessment instrument is optional for the HEI. However, it is worth mentioning that also non-EU countries might adapt their current data protection regulation in the future. For example, Switzerland is currently undergoing a review of the federal data protection law, and it is expected to show close similarities to GDPR (PwC, 2018). Therefore, compliance with GDPR will nevertheless be a good preparation for HEIs. On the other hand, if the outcome of this check is 'GDPR applies,' then the next step is to start with stage 2.

Stage 2: Conduct Detailed GDPR Assessment

In the second stage, a HEI must go through all the assessments in the intended order. The order of the assessments was chosen from the Irish checklist (Data Protection Commission, 2017) and will be explained in the following.

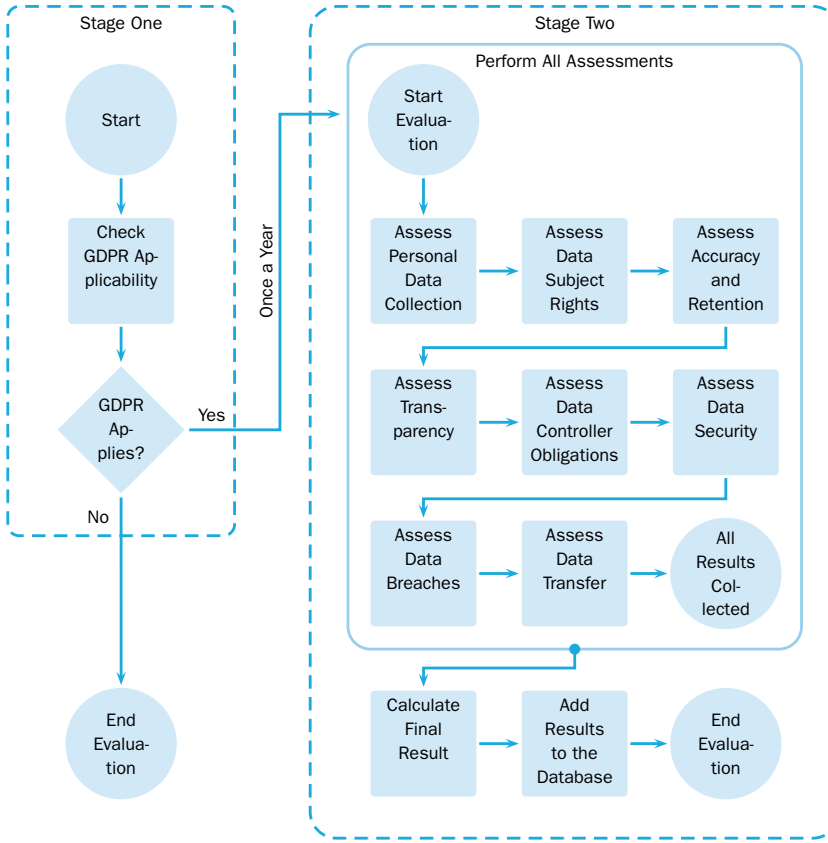


Figure 2 GDPR Assessment

Assess Personal Data Collection

In this process, several questions regarding the HEI's collection of personal data and corresponding lawful bases need to be answered. Initially, it is crucial to analyze which categories of GDPR-relevant personal data are concerned. Podnar (2017) proposes to evaluate whether visiting students from EU Member States are enrolled at the HEI or vice versa, and whether domestic students are spending a semester abroad at an EU higher education institution. In addition, professors, administrative, support or other EU staff working for the HEI should be considered. Cases where research funds from EU countries or donations from alumni students in the Union are received should be assessed as well.

Each processing of personal data needs to be based on legal ground, which could be a contract, legal obligations, and vital interests of the data subject, public interest, legitimate interest or consent (The European Parli-

Table 2 Assess Personal Data Collection

No.	Assessment question	Adapted from
Q1.5	Are consents, once obtained, appropriately documented and maintained?	ISACA (2018)
Q1.6	Does your HEI offer a way for individuals to withdraw their consent?	Data Protection Commission (2017)
Q1.7	Do you have documented and enforced privacy and security policies (and supporting procedures) to collect only the personal data that are adequate, relevant and limited to what is necessary in relation to the purposes for which the data are processed, in support of data-minimization requirements?	ISACA (2018)

ment and The Council, 2016, Art. 6). The latter case needs to meet special conditions (Art. 7). Any controller – the HEI in this case – must provide evidence of the data subject's (e.g., student's consent). This part of the GDPR assessment instrument is designed to assess the conditions for consent-based processing. Some example questions of this assessment are shown in Table 2.

Assess Data Subject Rights

One of the main objectives of GDPR is to provide individuals, the data subjects, with a wide array of rights that ensure the protection of their personal data. This part of the GDPR assessment instrument must ensure that a HEI has the correct procedures to cover the rights of data subjects as required by GDPR. It should be noted that these rights can be requested by any student, employee or other natural person in the EU from whom the HEI processes personal data and that the HEI should act within one month (The European Parliment and The Council, 2016, Art. 12). These rights are summarized in Table 3.

Assess Accuracy and Retention

According to UKs ICO (n.d.), the accuracy principle in GDPR promotes an obligation for organizations to take the appropriate steps to ensure the accurateness of the personal data they collect. GDPR did not define the term 'accurate.' However, according to the UK's Data Protection Act, 'inaccuracy' means that data is 'incorrect or misleading as to any matter of fact' (The National Archives, 2018, p. 122). Moreover, GDPR aims to ensure that the personal data that an organization keeps, where necessary, must be up to date (The European Parliment and The Council, 2016, Art. 5) and data subjects have the right to rectification (see Table 3). On the other hand, data must not be kept longer than it is required for any legal purpose (Art. 5). This means, that any HEI should familiarize itself with legal retention peri-

Table 3 GDPR Data Subject Rights

Right	Details
Right to be Informed	Data subjects, e.g., students, have 'the right to be informed about the collection and use of their personal data.' (ICO, n.d.)
Right of Access	Data subjects have the right to receive access to their own data and to obtain a copy from the HEI.
Right to Rectification	A HEI must rectify inaccurate data of students, employees and other natural persons from whom they process data on request.
Right to be Forgotten	Data subjects have the right to ask for deletion of their personal data, which the HEI needs to follow under certain circumstances (e.g., in case data is needed to comply with legal obligations such as a retention period, the law does not apply)
Right to Restrict Processing	In certain circumstances, such as the unlawfulness of data processing, the HEI is obliged to restrict the processing of personal data on the data subject's request.
Rights Related to Automated Decision Making	Data subjects, e.g., students, have 'the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.' (The European Parliment and The Council, 2016, Art. 22)
Right to Object	In certain circumstances, such as direct marketing a HEI might conduct, individuals have the right to object to the processing of their personal data.
Right for Data Portability	Data subjects must have the possibility to transfer their data to another HEI upon request.

Notes Questions adapted from Data Protection Commission (2017) and ISACA (2018).

Table 4 Assess Accuracy and Retention

No.	Assessment question	Adapted from
Q3.1	Do you have documented and enforced privacy and security policies (and supporting procedures) to ensure that personal data are kept accurate and up to date, as necessary, and to correct personal data errors without delay?	ISACA (2018)
Q3.4	Does your HEI have procedures in place to ensure personal data is destroyed securely, in accordance with your retention policies?	Data Protection Commission (2017)

ods for any personal data they store. Table 4 provides an extract of questions.

Assess Transparency

In this part of the GDPR assessment instrument, the openness and transparency requirements of GDPR are laid out. In simple terms, the students, employees and further data subjects of a HEI must be informed about the use of their personal data (Cormack, 2017). Additionally, a HEI must also inform its data subjects about their privacy rights 'in writing, or by other

Table 5 Assess Transparency

No.	Assessment question	Adapted from
Q4.2	Where personal data is collected directly from the individuals (such as students, alumni, researchers), are procedures in place to provide the information listed at Article 13 of the GDPR?	Data Protection Commission (2017)
Q4.3	Do you have documented and enforced policies (and supporting procedures and processes) to communicate to data subjects their rights, and answer their questions and provide information to them relating to data processing, in a manner that is clear, easy to understand, and age appropriate to the data subject (such as students, parents, researchers)?	ISACA (2018)

Table 6 Assess Controller's Obligations

No.	Assessment question	Adapted from
Q5.1	Have you published the contact details of your DPO to facilitate your students, employees or any other data subject in making contact with them?	Data Protection Commission (2017)
Q5.4	Does your HEI have agreements with suppliers and other third parties processing personal data on its behalf? If yes, have these agreements been reviewed to ensure all appropriate data protection requirements are included?	Data Protection Commission (2017)

means, including, where appropriate, by electronic means' (The European Parliment and The Council, 2016, Art. 12). Moreover, every HEI should have procedures to answer its students,' employees' and other individuals' requests regarding the personal data it withholds. A selection of questions to assess transparency can be found in Table 5.

Assess Controller's Obligations

There are other obligations that a HEI must consider when intending to become GDPR-compliant. One of these obligations is to investigate whether the HEI needs to assign a DPO or not. This part of the assessment instrument is divided into two sub-processes. The first process checks the necessity for a DPO assignment, while the second part checks other obligations such as agreements with suppliers, DPIAs, and the way a HEI handles the DPO if needed (see Table 6 for an extract of questions).

Assess Data Security

According to GDPR, it is the HEI's responsibility to secure its processing of personal data by means of 'appropriate technical and organizational measures' against damage, theft, or destruction (The European Parliment and The Council, 2016, Art. 5, 24). According to Article 32, there are several safeguards that every organization must consider when protecting the personal data it holds. One of these measures is pseudonymization, which

Table 7 Assess Data Security

No.	Assessment question	Adapted from
Q6.8	Can access to personal data be restored in a timely manner in the event of a physical or technical incident?	Data Protection Commission (2017)

is a technique that insists on protecting privacy by replacing real names or identifiers for data subjects (Tinabo, Mtenzi, & O'Shea, 2009). Another technique that is recommended by GDPR is the encryption of personal data. Moreover, GDPR states that it is the controller's – in our case the HEI's – responsibility to ensure the ability to restore and recover data in the event of damage, loss or physical incident (The European Parliament and The Council, 2016, Art. 5, 32). Table 7 shows a sample question belonging to this part of the assessment instrument.

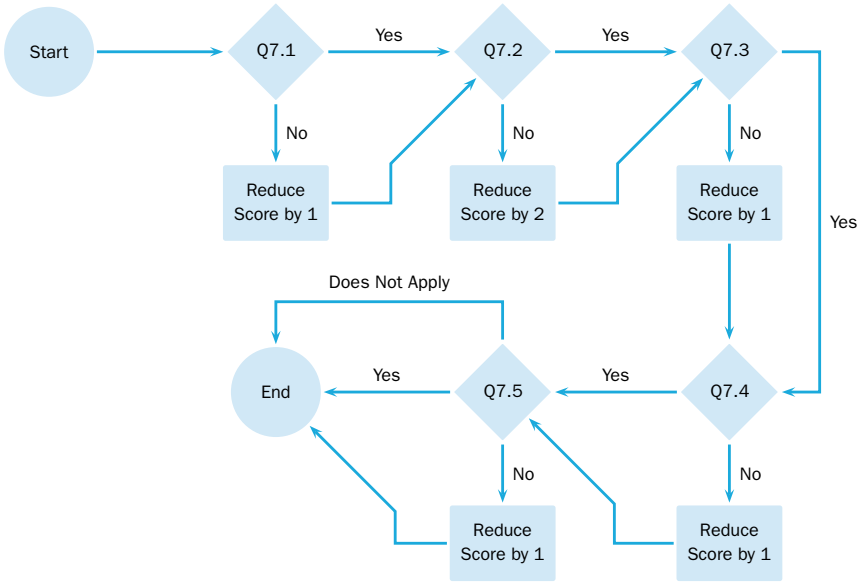
Assess Data Breaches

GDPR introduces an obligation of organizations to notify data subjects and relevant supervisory authorities in case of a personal data breach likely to result in a risk to the rights and freedoms of natural persons (The European Parliament and The Council, 2016, Art. 33). This notification must take place within the first 72 hours of its discovery (Tankard, 2016). Therefore, a HEI must have a documented plan that includes the GDPR requirements for data breach policies. According to ICO (n.d.), preparing a data breach plan entails: (1) Knowledge of how to detect a data breach. (2) Understanding of what is classified as a data breach, for example, students' grades qualify as breached in many cases. (3) A response plan for addressing breaches if they occur. (4) Allocation of responsibility to a designated person to manage breaches. (5) Awareness of the staff of escalating any incident to the designated person. These considerations result in specific checks for HEIs outlined in Figure 3.

Assess Data Transfer

If a Swiss HEI transfers personal data to any party outside the EU, e.g., partner universities to support exchange semesters, many conditions must be applied under the GDPR. Examples are:

- The foreign university or other partner must be in a country that ensures an 'adequate' level of protection (The European Parliament and The Council, 2016, Art. 45). Although the term 'adequate' is not explicitly defined, there are some controls for assessing the level of protection, such as the rule of law, or human rights in the country of processing, i.e. the country of the partner university in this case. It is



Q7.1 Does your HEI have a policy to define what is considered a data breach?
Q7.2 Does your HEI have a response plan to data breaches?
Q7.3 Does this plan ensure notifying the supervisory authority within 72 hours if a breach takes place?
Q7.4 Are all data breaches fully documented?
Q7.5 Is there any cooperation with other partners to deal with data breaches?

Figure 3 Visualization of 'Assess Data Breaches' Part of the GDPR Assessment Instrument for HEIs (Adapted from Data Protection Commission, 2017; ISACA, 2018; Varankevich, 2017)

recommended to check for any 'adequacy decisions' made by the EU Commission (ICO, n.d.)

- The HEI must implement safeguards to ensure the minimization of risks that surrounds the transfer of personal data (ICO, n.d.). According to Tikkinen-Piri et al. (2018), safeguards do either not require any specific authorization from a supervisory authority (such as standard data protection clauses adopted by the European Commission) or they can be used based on an authorization (for example, in case transfers are based on contractual clauses between the controller or the processor and the recipient).

This is the final check of the GDPR assessment instrument. It questions the user's HEI about the previous conditions along with some other requirements such as the documentation of data transfers (see a selection of questions in Table 8).

Table 8 Assess Data Transfers

No.	Assessment question	Adapted from
Q8.1	Does your HEI transfer data outside the European Economic Area? If yes, are all personal data transfers documented?	Data Protection Commission (2017)
Q8.4	Are data subjects fully informed about any intended international transfers of their personal data?	Data Protection Commission (2017)

Assessment Results

Answering all of the GDPR assessment instrument's questions and tracking the process models leads to a final assessment result. The prototype version is designed to let a HEI start with a score of 44 points and end up with a resulting number between 0 to 44. As it becomes visible in Figure 3, any answer that indicates non-compliance with a GDPR regulation leads to a score deduction, which might be weighted with one or several points. It is important to stress what this overall assessment score should not indicate: it should not express a dedicated level of compliance, such as being 'half or two third compliant.' Instead, if the assessment is conducted on a regular basis, the overall score is an estimation that supports the progress a HEI has made on its GDPR journey.

Conclusion and Outlook

The contribution of this study is the development of a prototype for a GDPR assessment instrument that can be used by HEIs in Switzerland, but also by other HEIs residing in a non-EU state, to provide an insight into a HEI's GDPR readiness (represented as a total score).

The prototype is intended to be a supporting instrument for experienced users in the field of data protection or DPOs when they carry out a low-threshold assessment in connection with GDPR requirements. Overall, the complete prototype consists of the following parts: firstly, an Excel-based sheet that contains all the questions of the assessment instrument numbered and colour-coded to match their respective process models. Secondly, a document is provided containing all the assessments of the two stages in the form of graphical process models, which is used to guide through the assessment. Finally, the prototype was tested and evaluated by compliance and modelling experts who concluded that the prototype is useful and can be used by data privacy personnel to assist any DPO in getting an overview of a HEIs readiness for GDPR.

Since this study is the first iteration of the development of the instrument, it is possible that some improvement could take place in the future. Several amendments were suggested by the participants of the evaluating

workshop and should be taken into account in future developments such as digitizing the instrument and further evaluating the instrument based on lawyers' expertise. Moreover, GDPR deals with the protection of the data of European citizens, regardless of whether the organization generates profit from its data processing or not. As a potential further expansion, since this study deals with HEIs in an abstract way, the instrument could be adapted and generalized to fit any non-profit organization.

References

Albrecht, J. P. (2017). How the GDPR will change the world. *European Data Protection Law Review,* 2(3), 287–289.

BayLDA. (n.d.). Weg zur DS-GVO – Selbsteinschätzung. Retrieved from https://www.lda.bayern.de/tool/start.html

Cormack, A. (2017, 24 May). A year to get your act together: How universities and colleges should be preparing for new data regulations. Retrieved from www.jisc.ac.uk/blog/a-year-to-get-your-act-together-how-universities-and-colleges-should-be-preparing-for-new-data-regulations

Data Protection Commission. (2017). *Preparing your organisation for the general data protection regulation.* Retrieved from http://gdprandyou.ie/wp-content/uploads/2017/12/A-Guide-to-help-SMEs-Prepare-for-the-GDPR.pdf

Ebert, N., & Widmer, M. (2018). *Datenschutz in schweizer unternehmen 2018: Eine Studie des Instituts für Wirtschaftsinformatik und des Zentrums für Sozialrecht.* Retrieved from https://digitalcollection.zhaw.ch/bitstream/11475/11382/3/2018_Ebert%20Datenschutz%202018.pdf

Economiesuisse. (n.d.). Datenschutz 'Online Check.' Retrieved from www.economiesuisse.ch/de/datenschutz-online-check

European Court of Human Rights. (2018). *Guide on article 8 of the European Convention on Human Rights.* Retrieved from www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf

Garber, J. (2018). GDPR-compliance nightmare or business opportunity? *Computer Fraud & Security,* No. 6, 14–15.

Hevner, A. R., & Chatterjee, S. (2010). Design science research in information systems. In *Design research in information systems* (pp. 9–22). Boston, MA: Springer.

Hevner, A. R., Salvatore T. M., Jinsoo P., & Sudha R. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105.

ICO. (n.d.). Guide to the General Data Protection Regulation (GDPR). Retrieved from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr

ISACA. (n.d.). ISACA CMMI GDPR assessment. Retrieved from www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ISACA-CMMI-GDPR-Assessment.aspx.

ISACA. (2018). GDPR Assessment. Retrieved from https://gdprassessment.isaca.org

Krystlik, J. (2017). With GDPR, preparation is everything. *Computer Fraud and Security,* No. 6, 5–8.

Lurati, N. (2018, 13 September). Auch kleine Schweizer Webshops müssen aufpassen. Retrieved from https://www.blick.ch/news/politik/die-neue-eu-daten-schutzverordnung-betrifft-fast-alle-auch-kleine-schweizer-webshops-muessen-aufpassen-id8444056.html.

Microsoft. (2018). *GDPR for Education.* Retrieved from https://pulse.microsoft.com/uploads/prod/2018/03/WorkProductivity_GDPRforEducation_KickStartGuide.pdf

Müller, G. V. (2017, 14 July). Die positiven Seiten der Regulierung. https://www.nzz.ch/meinung/eu-datenschutz-und-die-schweiz-die-positiven-seiten-der-regulierung-ld.1305966

Podnar, K. (2017, 21 September). Is your university ready to pass the GDPR exam? Retrieved from https://medium.com/kpodnar/is-your-university-ready-to-pass-the-gdpr-exam-eac6641cebbc

PwC. (2018). Was bringt die Revision des Schweizer Datenschutzgesetzes mit sich und wie hängt dies mit der DSGVO und der ePrivacy-Verordnung zusammen? Retrieved from https://www.pwc.ch/de/publications/2018/Datenschutz_in_der_Schweiz.pdf

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students.* Harlow: Prentice Hall.

Segarra, L. (2018, 24 March). Mark Zuckerberg lost $10 billion after Cambridge Analytica. Retrieved from http://money.com/money/5213181/mark-zuckerberg-lost-10-billion-in-one-week-after-facebooks-privacy-scandal/

Tankard, C. (2016). What the GDPR means for businesses. *Network Security,* No. 6, 5–8.

The European Parliment and The Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *Official Journal of the European Union,* L 119/1–88.

The National Archives. (2018). Data Protection Act 2018. Retrieved from www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review 34*(1), 134–153.

Tinabo, R., Mtenzi, F., & O'Shea, B. (2009, November). *Anonymisation vs. pseudonymisation: Which one is most useful for both privacy protection and usefulness of e-healthcare data.* Paper presented at the 2009 International Conference for Internet Technology and Secured Transactions, London, England.

Varankevich, S. (2017, 17 february). Territorial scope of the GDPR (Flowchart). Retrieved from www.linkedin.com/pulse/territorial-scope-gdpr-flowchart-siarhei-varankevich

Wong, J. C. (2019, 22 March). Facebook acknowledges concerns over Cambridge Analytica emerged earlier than reported. Retrieved from https://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing

Ali Habbabeh is a Master's student at the University of Applied Sciences and Arts Northwestern Switzerland and research assistant at the Competence Center Blockchain. He chose data protection as his bachelor thesis topic. Skilled in software engineering and passionate for new technologies, one of Ali Habbabeh's newly arising research areas is Smart Contracts governance in the area of Blockchain. *ali.habbabeh@fhnw.ch*

Bettina Schneider is researcher and lecturer at the Competence Center Cyber Security and Resilience at the University of Applied Sciences and Arts Northwestern Switzerland, School of Business. She obtained her PhD in the field of Information Systems and Education in 2016. In her recent research, she focuses on Privacy and Cyber Security, Integrated Business Systems, as well as Education. *bettina.schneider@fhnw.ch*

Petra Maria Asprion is researcher and lecturer at the University of Applied Sciences and Arts Northwestern Switzerland, School of Business. She is the Head of the Competence Center Cyber Security and Resilience, as well as Blockchain. *petra.asprion@fhnw.ch*