SQELT PROJECT

SUSTAINABLE QUALITY ENHANCEMENT IN HIGHER EDUCATION LEARNING AND TEACHING. Integrative Core Dataset and Performance Data Analytics

Co-funded by the Erasmus+ Programme of the European Union

Key Action: **Cooperation for innovation and the exchange of good practices**
Action Type: **Strategic Partnerships for higher education**

Partners: EVALUATION AGENCY BADEN-WUERTTEMBERG, UNIVERSIDADE DE AVEIRO, BIRMINGHAM CITY UNIVERSITY, UNIVERSITEIT GENT, UNIWERSYTET JAGIELLONSKI, UNIVERSITÄT FUR WEITERBILDUNG KREMS, UNIVERSITEIT LEIDEN, UNIVERSITÀ DEGLI STUDI DI MILANO, UNIVERSITETET I OSLO, CENTRO DE INVESTIGAÇÃO DE POLÍTICAS DO ENSINO SUPERIOR

https://www.evalag.de/sqelt/
https://ec.europa.eu/programmes/erasmus-plus/projects/eplus-project-details/#project/b8a93e06-2000-4a82-9fac-90b3bcacadec

Intellectual Output O8:

ETHICAL CODE OF PRACTICE FOR (PERFORMANCE) DATA MANAGEMENT[1]

Project coordinator/Contact person:
Prof. Dr. Dr. Theodor Leiber
Sect. 3: Science Support, **evalag** (Evaluation Agency Baden-Wuerttemberg)
PO Box 120522, D-68056 Mannheim, Germany
Tel 0621-12854525, leiber@evalag.de
http://www.evalag.de/

30 September 2020

The creation of this resource has been (partially) funded by the ERASMUS+ grant program of the European Union under grant no. 2017-1-DE01-KA203-003527. Neither the European Commission nor the project's national funding agency DAAD can be held responsible for the content or liable for any losses or damage resulting of the use of this resource.

[1] For reasons of content, the title of Intellectual Output O8 has been changed from "Comprehensive Ethical Code of Practice for Learning Analytics" in the SQELT Application to "Ethical Code of Practice for Data Management".

Content

EXECUTIVE SUMMARY

According to the increasing pervasiveness of data and analytics, such as learning analytics, academic analytics, research analytics, strategy analytics, there still exists increasing interest in the definition, measurement and justified use of performance data in higher education ranging from research through learning and teaching (L&T) to third mission. In practice and theory of performance data use, the ethics of why and how which data are collected and used is a core issue: higher education institutions (and other social organisations as well) are required to develop ethical codes of practice for (performance) data management and to adopt them explicitly as part of their governance approach. This need is further enforced by the fact that various legal or regulatory requirements already exist for handling data and information at national, European and international levels, that must be observed by higher education institutions.

However, so far not very many universities have addressed ethical issues in their comprehensive complexity at the organisational levels. Therefore, it is important for any higher education institution to develop clear principles and guidelines on ethical data use. The guidance thus given must be guidance for institutions and individuals including the technology systems and applications. Although, the responsibility for data ethics ultimately rests with an organisation's leadership, ethical behaviour in collecting, accessing, interpreting and using data, particularly education data, is the responsibility of every individual member of an educational organisation. Among these involved stakeholders constituting the data ethics audience are teaching staff; students; data quality management staff; information systems staff; leadership in all relevant areas on all organisational levels. To make this a reality, comprehensive organisational structures and practices must be established which encourage ethical conduct.

Against this backdrop, this Ethical Code of Practice for Data Management (ECPDM) clarifies who and what this ECPDM applies to. Then, seven ethical principles of data management are presented, six moral and lawful bases for data management are characterised and eight individual rights related to data management are described. Based on these considerations and institutional case studies giving an overview of the development status of data ethics at six European universities, the following insights and recommendations emerge: The six partnership universities – University of Aveiro (UA); Birmingham City University (BCU); University Ghent (UGhent); Jagiellonian University in Krakow (JU); Danube University Krems (DUK); University of Milan (UNIMI) – already achieved to implement most of the General Data Protection Regulation (GDPR) principles, thus compliance being high with GDPR and national law that ensures GDPR enforcement. All partnership universities have an institutional digitalised information and data system. The majority of universities has important constituents of ethical data management (in L&T) in place. Thus, the universities identify several strengths but also weaknesses, opportunities and threats.

Omnipresent weaknesses reported by all partnership universities are deficiencies in dissemination and implementation of good data ethics conduct ("institution-wide quality culture of data ethics") and the practical incompleteness of institutional digitalised information and data systems. The case studies further show that three main opportunities exist that can be helpful for overcoming the identified weaknesses and avoid the threat(s): Improve on compliance with ECPDM and thus improve on compliance with GDPR; learn from national and international ethical codes of practice for data management; learn from national legislation on information and data management. The big threats that the SQELT partnership universities see are the following: There is always the risk of hacker attacks to the university's digitalised information and data system. Another omnipresent risk is the unduly use of data that breaches the GDPR and this ECPDM.

INTRODUCTION AND OVERVIEW

Many new opportunities to support and enhance performance of organisations, among them the multiple-hybrid organisations called 'higher education institutions' (cf. Kleimann 2019; Leiber 2019), emerge from the increasing pervasiveness of data[2] and analytics (such as learning analytics, academic analytics, research analytics, strategy analytics). Accordingly, there still exists increasing interest in the definition, measurement and justified use of performance data in higher education ranging from research through learning and teaching (L&T) to third mission. However, a major issue that is said to be very important by many but nevertheless often neglected in practice and theory is the ethics of why and how which data are collected and used. These facts as well as the growing public awareness because of numerous data abuse scandals require higher education institutions (and other social organisations as well) to develop ethical codes of practice for (performance) data management and to adopt them explicitly as part of their governance approach. This need is also reinforced by the fact that various legal or regulatory requirements already exist for handling data and information at national, European and international levels (e.g. the European General Data Protection Regulation (EC 2016); Intellectual Property Rights; Privacy Rights; Constitutional Rights related to information and data use; see also NFES 2010, p. 41ff.), that must be observed by higher education institutions.

The ethical considerations underpinning the collection and use of performance data in higher education and the design of analytics systems that will use this data are complex. Not least, this should be one of the reasons why so far not very many universities have addressed ethical issues in their comprehensive complexity at the institutional, organisational level. Therefore, it is important for any higher education institution to develop clear principles and guidelines on ethical data use. The guidance thus given must be guidance for institutions and individuals including the technology systems and applications. In particular, the technical possibilities themselves should not determine the ethical principles and standards of measuring, collecting and using data, but rather the critical-ethical reflections of users and those affected. Hereby, the very basics of ethics are fundamentally geared towards avoiding or reducing evils and increasing benefits.

This approach to data ethics focuses on (though is not restricted to) L&T in higher education simply for pragmatic reasons: it was developed in the framework of the Erasmus+ project "**S**ustainable **Q**uality **E**nhancement in Higher Education **L**earning and **T**eaching" (SQELT) with an operational time of 33 months (SQELT 2020), and there is plausibility in focusing on one sub-area of data ethics because of its broad scope and complexity.

General insights from quality enhancement suggest that the following policies shall be followed when developing and establishing a data ethics framework for L&T at an education institution:

- Actively engage with multiple stakeholders, in particular students and staff, to establish transparency, commitment and trust by discursive inclusion and participation;
- Avoid reinventing the wheel, instead use and further develop and improve existing approaches;
- Keep the data ethics framework open for revisions and improvement in the light of critical feedback and future technology development.

Against this backdrop, this Ethical Code of Practice for Data Management (ECPDM) is mainly informed by and based on the following sources:

- The European General Data Protection Regulation (GDPR) (EC 2016)
- *The Ethics of Learning Analytics in Australian Higher Education* (Corrin et al. 2019)
- *Guide to the General Data Protection Regulation* (ICO 2019)
- *Learning Analytics Explained* (Sclater 2017)
- *Code of Practice for Learning Analytics* (Sclater 2014)
- *The Forum Guide to Data Ethics* (NFES 2010)
- Six institutional SQELT case studies about data ethics in higher education L&T, see Appendix 1

[2] For the present purposes, the notion of "data" is meant to comprise quantitative data as well as qualitative information.

Hereby, the GDPR takes a rather prominent role because the SQELT ECPDM shall be in accordance with the GDPR of the European Union (EU). Furthermore, according to the comparative analyses of various approaches by the SQELT Strategic Partnership group the GDPR seems a relevant and reliable approach which comprises and synthesizes several relevant documented efforts in this respect.

Although, the responsibility for data ethics ultimately rests with an organisation's leadership, ethical behaviour in collecting, accessing, interpreting and using data, particularly education data, is the responsibility of every individual member of an educational organisation involved in the just mentioned data processing. Among these involved stakeholders constituting the data ethics audience are teaching staff; students; data quality management staff; information systems staff; leadership in all relevant areas on all organisational levels.

To make this a reality, organisational structures and practices must be established which encourage ethical conduct. Therefore,

> 'organisations must actively ensure that all data handlers adhere to all policies and procedures related to data ethics. Good communication throughout the organisation and effective training can go a long way to foster this culture. To help data handlers understand and exhibit standards of ethical behaviour, education organisations should: train staff about their ethical responsibilities; publicise the expectations for ethical behaviour; create explicit policies and procedures pertaining to data ethics; state clearly the consequences of unethical behaviour; and enforce these rules uniformly so that everyone is accountable. Ethics training requires a resource commitment from school leaders: securing skilled trainers, tailoring curricula to the organization's and learners' needs, and allocating professional development time for staff to learn and practice new behaviours. In addition to describing ethical concepts, training should discuss why ethics matter (ethical issues are real and have significant consequences) and how ethics play out in everyday situations in the organization (that is, how they affect the routine activities of the training participants)' (NFES 2010, p. 3).

This ECPDM is organised as follows: the first section clarifies who and what this ECPDM applies to. In the second section seven ethical principles of data management are presented. Section three characterises six moral and lawful bases for data management while section four describes eight individual rights related to data management. The ECPDM closes with common insights and recommendations. All these themes and issues are presented with a focus on but are not restricted to personal data in higher education since many issues also apply to non-personal data and organisations outside higher education institutions.

Further, Appendix 1 presents six institutional SQELT case studies giving an overview of the development status of data ethics with respect to Ethical Principles of Data Management, Moral and Lawful Bases for Data Management and Individual rights Related to Data Management at the six partnership universities, University of Aveiro, Birmingham City University, Ghent University, Jagiellonian University in Kraków, Danube University Krems and University of Milan. Finally, Appendix 2 gives a Project Workbook Framework on Data Ethics (PWFDE) that complements the Ethical Code of Practice for Data Management (ECPDM). The PWFDE refers to ECPDM and provides a framework for ethics of data management to be offered to and applied by projects that comprise (personal) data protection issues. The function of PWFDE is to help optimise projects regarding data protection and alignment with GDPR and ECPDM.

CONDITIONS OF APPLICATION OF THIS ETHICAL CODE

Types of actors and their ethical and legal obligations regarding personal data

Following the GDPR, this Ethical Code of Practice for Data Management (ECPDM) applies to 'controllers' and 'processors' insofar they are dealing with personal data, i.e. data of individual, natural persons. (This does not rule out that many of the following principles and rules also apply to the handling of non-personal data.) A controller determines the purposes and means of processing data while a processor is responsible for processing data on behalf of a controller.

Again, following the GDPR this ECPDM refers to specific moral and legal obligations on processors and controllers of personal data. For example, processors are required to maintain records of personal data and

processing activities and have legal liability if responsible for a data security breach, while the controllers' contracts with processors shall comply with this code of practice.

In the spirit of the GDPR this ECPDM also applies to data processing carried out by higher education institutions (HEIs) and similar organisations operating within the European Higher Education Area (EHEA) being part of the European Economic Area (EEA) as well as organisations outside the EHEA that offer goods or services to individuals in the EHEA.

However, this ECPDM does not apply to certain activities including data processing covered by Law Enforcement Directives, processing for national security purposes and processing carried out by individuals purely for personal/household activities.[3]

The concept of personal data

Any information and data that may support (together with other information) the identification of an individual (i.e. a natural person) counts as 'personal data', if it 'relates to' this individual (also called 'data subject'), for example, because it contains specific information about the individual and could have an impact on the individual. The identification of an individual can take place by the following factors: name; identification number; location data; online identifiers (e.g. IP address; cookie identifier); or other factors.

There are several other features that characterise the concept of personal data among them the following: Due to the possible interaction of different data it is possible that the same information is personal data for one controller's purposes but is not personal data for the purposes of another controller. Furthermore, information which has had identifiers removed or replaced to pseudonymise the data is still personal data. By contrast, information which is truly anonymous is not covered by this ECPDM. Information, that seems to relate to a particular individual, counts as personal data even if it is inaccurate (for example, if it is factually incorrect or is about a different individual). Also, information about individuals acting as sole traders, employees, partners and company directors where they can be individually identified and the information relates to them as an individual may constitute personal data. However, the following type of data does not count as personal data in the sense of GDPR and therefore ECPDM: information about a deceased person; information about companies or public authorities.[4]

ETHICAL PRINCIPLES OF DATA MANAGEMENT

Following GDPR and related regulations and analyses (cf. Corrin et al. 2019; EC 2016; Sclater 2014; Sclater 2017; Tranberg et al. 2018), this ECPDM advocates the following seven ethical principles of data management[5]:

Lawfulness, fairness and transparency

This means that data, particularly personal data, shall be 'processed lawfully, fairly and in a transparent manner in relation to the data subject' (EC 2016, p. 35).

Purpose limitation

This means that data, particularly personal data, shall be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall […] not be considered to be incompatible with the initial purposes' (EC 2016, p. 35).

[3] Relevant provisions for the above considerations in the GDPR are: Articles 3, 28-31 and 49 (EC 2016).
[4] Relevant provisions for the above considerations in the GDPR are: Articles 2, 4, 9 and 10 (EC 2016).
[5] Relevant provisions for the following considerations in the GDPR are: Articles 5(1) and 5(2) (EC 2016). Generally, the seven ethical principles are relevant for any data management and not exclusively for the management of personal data. The principles are relevant for this ECPDM for their strong ethical reference. At the same time, however, these principles also refer to methodological issues. This means that ethical and methodological aspects and dimensions are not completely separable, even not on the level of the most basic ethical principles (also cf. Leiber & Meyer 2019).

Data minimisation

This means that data, particularly personal data, shall be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed' (EC 2016, p. 35).

Accuracy

This means that data, particularly personal data, shall be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay' (EC 2016, p. 35).

Storage limitation

This means that personal data shall be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes […] subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of individuals' (EC 2016, p. 36).

Integrity and confidentiality (security)

This means that personal data shall be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures' (EC 2016, p. 36).

To achieve this, tools like risk analysis and organisational policies are required. Where appropriate, measures such as 'pseudonymisation and encryption of personal data' (EC 2016, p. 51) should be used 'to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services' (EC 2016, p. 52). The measures must also enable controllers and processors 'to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident' (EC 2016, p. 52). There must be appropriate processes in place to test the effectiveness of applied measures, and undertake any required improvements (EC 2016, p. 52).[6]

Accountability/responsibility

This means that the controller is responsible for all six ethical principles of (personal) data management listed above and can demonstrate compliance with them (EC 2016, p. 36): lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality.

To implement accountability or responsibility, controllers and processors need to put in place appropriate technical and organisational measures, including, among others, the following options[7]:

- They need to maintain documentation of personal data processing activities (a must);
- They need to appoint a data protection officer (a must);
- They need to review and, where necessary, update the accountability measures put in place (a must);
- They need to have written contracts with organisations that process personal data on their behalf;
- They need to adopt and implement data protection policies including a privacy management framework to support embedding accountability measures and creating a culture of privacy across the organisation;
- They need to take a 'data protection by design and default' approach;

[6] Relevant provisions for this in the GDPR are: Article 32(1) (EC 2016).
[7] Relevant provisions for this in the GDPR are: Articles 12-14, 22, 24(1), 33, 34, 58 and 83 (EC 2016).

- They need to record and, where necessary, report personal data breaches within three calendar days of becoming aware of the breach, where feasible; if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must also be informed without undue delay;
- They need to conduct data protection impact assessments for uses of personal data that can pose a high risk to the interests of individuals (a must for data processing likely to result in a high risk);
- They should implement appropriate security measures;
- They should keep a record of any personal data breaches, regardless of whether it is required to notify;
- They should ensure that robust breach detection, investigation and internal reporting procedures are in place to facilitate decision-making about whether or not the relevant supervisory authority and the affected individuals need to be notified;
- They should adhere to relevant codes of conduct and sign up to certification schemes.

MORAL AND LAWFUL BASES FOR DATA MANAGEMENT

Following the GDPR (EC 2016, Article 6), this ECPDM sets out six "moral and lawful bases" for the processing of data related to individuals. Accordingly, at least one of these must apply whenever personal data shall be processed.

This is of particular importance when special category data are concerned.[8] In such cases, it must be paid with increased precision to the compliance with the moral and lawful bases requirements. Examples of special category data are: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

These six moral and lawful bases are the following:

Consent

This case occurs when the individual data subject has given clear consent for the data processor and/or controller to process their personal data for a specific purpose. Clear consent means offering individuals real choice and control, i.e. it requires an explicit, positive opt-in. For example, the use of pre-ticked boxes or any other method of default consent is not allowed; consent requests shall be clearly separated from other terms and conditions.

The GDPR's high standards for consent further include that any third party controllers who will rely on the consent shall be named; it shall be made easy for people to withdraw consent and they should be told how; evidence shall be kept of the consent procedure (who, when, how, what); consent shall be kept under review, and refreshed if anything changes; consent to data processing shall not be made a precondition of a service.[9]

Contract

This case occurs when the data processing is necessary for a contract the data processor and/or controller has with the individual data subject, or because they have asked the individual to take specific steps before entering into a contract.

Whenever a controller uses a processor, there must be a written contract (or other legal act) in place which secures that both parties understand their responsibilities and liabilities. If a processor uses another organisation (i.e. a sub-processor) to assist in its processing of personal data for a controller, it needs to have a written contract in place with that sub-processor. The following information needs to be included in such

[8] Relevant provisions for this in the GDPR are: Article 9(21) (EC 2016).
[9] Relevant provisions for the above considerations in the GDPR are: Articles 4(11), 6(1)(a), 7, 8, 9(2)(a) (EC 2016).

contracts: subject matter of the processing; duration of the processing; nature and purpose of the processing; type of personal data involved; categories of data subject; controller's obligations and rights.[10]

Legal obligation

This case occurs when the data processing is necessary for the data processor and/or controller to comply with the law (not including contractual obligations).[11] A relevant example is data processing in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of data subjects.

Vital interests

This case occurs when the data processing is necessary to protect someone's life.[12]

Public tasks

This case occurs when the data processing is necessary for the data processor and/or controller to perform a task in the public interest or for their official functions, and the task or function has a clear basis in law.[13]

Legitimate interests

This case occurs when the data processing is necessary for the legitimate interests of the data processor and/or controller or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if the data processor and/or controller are public authorities processing data to perform their official tasks.) Legitimate interests can include commercial interests, individual interests or broader societal benefits.

Legitimate interests is the most flexible lawful basis for data processing, though it may not always be the most appropriate. It is likely to be most appropriate where individuals' data are used in ways they would reasonably expect, with little privacy impact, or if there is a compelling justification for the processing of the data. If the individuals would not reasonably expect the data processing, or if it would cause unjustified harm, the individuals' interests are likely to override an organisation's legitimate interests. Details of an organisation's legitimate interests need to be included in their privacy information.[14]

INDIVIDUAL RIGHTS RELATED TO DATA MANAGEMENT

In accordance with the GDPR this ECPDM provides the following eight distinguishable rights for individuals with reference to the management of data related to them[15]:

The right to be informed

The individuals have the right to be informed about the collection and use of their personal data (GDPR key transparency requirement).

Therefore, the individuals must be supplied with information including: the purposes for the processing of their personal data, the retention periods for this personal data, and with whom it is shared ('privacy information'). In general, privacy information must be provided to individuals at the time their personal data is collected. If personal data are obtained from other sources, however, individuals (data subjects) must be provided with privacy information within a reasonable period of obtaining the data and, according to GDPR, no later than one month.

[10] Relevant provisions for the above considerations in the GDPR are: Articles 6(1)(b) (EC 2016).
[11] Relevant provisions for the above considerations in the GDPR are: Article 6(1)(c) (EC 2016).
[12] Relevant provisions for the above considerations in the GDPR are: Article 6(1)(d), 9(2)(c) (EC 2016).
[13] Relevant provisions for the above considerations in the GDPR are: Article 6(1)(e), 6(3) (EC 2016).
[14] Relevant provisions for the above considerations in the GDPR are: Article 6(1)(f) (EC 2016).
[15] Relevant provisions in the GDPR are: Article 10 (EC 2016).

Among others, the following exceptions of the data subject's right to be provided with privacy information exist: an individual already has the information; providing the privacy information would involve a disproportionate effort.

In accordance with the ethical principle of accuracy, the privacy information provided to data subjects shall be concise, transparent, intelligible, easily accessible, and it shall use clear and plain language. Privacy information shall be regularly reviewed, and where necessary, updated.[16]

The right of data access

Individuals have the right to access their personal data ('subject access').

Individuals can make a subject access request verbally or in writing. The controller or processor has one calendar month to respond to a subject access request. The controller or processor cannot charge a fee to deal with a request in most circumstances.[17]

The right to data rectification

Individuals have the right to have inaccurate personal data rectified or completed if it is incomplete.

Individuals can make a request for rectification verbally or in writing. The controller or processor has one calendar month to respond to a request. In certain circumstances the controller or processor can refuse a request for rectification.[18]

The right to data erasure

Individuals have the right to erasure of their personal data ('right to be forgotten').

Individuals can make a request for erasure verbally or in writing. The controller or processor has one calendar month to respond to a request.[19]

The right to restrict data processing

Individuals have the right to request the restriction or suppression of processing of their personal data.

When data processing is restricted, the controller or processor are permitted to store the personal data, but not use it. An individual can make a request for restriction verbally or in writing. The controller or processor has one calendar month to respond to a request.[20]

The right to data portability

Individuals have the right to data portability of their personal data.

The right to data portability allows individuals to securely and reliably receive (i.e. move, copy, transfer) and reuse their personal information for their own purposes across different services and IT environments. The right to data portability only applies to information an individual has provided to a controller.[21]

The right to object data processing

Individuals have the right to object to the processing of their personal data.

---

[16] Relevant provisions for the above considerations in the GDPR are: Articles 12-14 (EC 2016).
[17] Relevant provisions for the above considerations in the GDPR are: Articles 12 and 1 (EC 2016).
[18] The right to data rectification is closely linked to the controller's and processor's obligations under the ethical accuracy principle which is based on Article 5(1)(d) of the GDPR (EC 2016); relevant provisions for the above considerations in the GDPR are: Articles 5, 12, 16 and 19 (EC 2016).
[19] Relevant provisions for the above considerations in the GDPR are: Articles 6, 9, 12 and 17 (EC 2016).
[20] The right to restrict data processing is closely linked to the right to data rectification and the right to object data processing which are based on Articles 16 and 21 of the GDPR, respectively (EC 2016); relevant provisions for the above considerations in the GDPR are: Articles 6, 9, 12 and 17 (EC 2016).
[21] Relevant provisions for the above considerations in the GDPR are: Articles 13 and 20 (EC 2016).

In the case of data being used for direct marketing data subjects have an absolute right to stop this practice. In other cases where the right of objection applies, data controllers and processors may be able to continue processing if they can prove that they have a compelling reason for doing so.

Individuals can make an objection to personal data processing verbally or in writing. The controllers and processors have one calendar month to respond to an objection. Data controllers need to inform data subjects about their right to object.[22]

Rights in relation to automated decision-making and profiling

Individuals have rights related to automated decision-making based on their personal data including profiling.

Accordingly, solely automated decision-making based on their personal data shall only be carried out if the decision is necessary for the conclusion or performance of a contract, or in accordance with Union law or the law of a Member State applicable to the controller, or based on the expressed consent of the individual.

Controllers and processors must identify their automated decision-making processes and inform individuals about the data processing, introduce simple ways for individuals to request human intervention or challenge a decision, and carry out regular checks to make sure that their systems are working as intended.[23]

INSIGHTS AND DEVELOPMENT OPTIONS FROM THE SQELT CASE STUDIES

In this section, insights and development options concerning ethics and practice of information and data management at the six partnership universities of the SQELT project are presented. They are drawn from the short SQELT case studies about data ethics in learning and teaching at the six partnership universities (see Appendix 1) as well as from additional information of the universities that have been gathered throughout the SQELT project.

The analysis reveals that the six partnership universities – University of Aveiro (UA); Birmingham City University (BCU); University Ghent (UGhent); Jagiellonian University in Krakow (JU); Danube University Krems (DUK); University of Milan (UNIMI) – already achieved to implement most of the GDPR principles, thus compliance being high with GDPR and national law that ensures GDPR enforcement. All partnership universities have an institutional digitalised information and data system. The compliance with GDPR implies that the ethics and practice of information and data management at the six partnership universities is in accordance with this Ethical Code of Practice for Data Management (ECPDM) as presented above. Particularly, the universities advocate and stand in for the relevant ethical principles, moral and lawful basis and individual rights related to data management (see Table 1; also cf. Appendix 1).

Further strengths identified at majority of the partnership universities are the availability of a Code of Ethics/Code of Conduct/Ethical guidelines on data management at institutional level; the existence of an Institutional Council of Ethics of Data Management; the implementation of a Data Protection Officer; the implementation of networks of unit pivots for ethical data management; the explicit engagement of the Rectorate to improve on the ethics of institutional data management. The incorporation of the data ethics topic in the university statutes is reported by only a minority of partnership universities (see Table 1).

Among the weaknesses with respect to ethics and practice of information and data management at the six partnership universities of the SQELT project are the following: one partnership university explicitly diagnoses the lack of an institutional Code of Ethics for Data Management, an institutional Code of Conduct for Data Management and an institutional policy of privacy and protection of personal data. Another partnership university reports the lack of documents for data protection regulation that transfer the GDPR to specific L&T topics (see Table 1).

So to speak omnipresent weaknesses reported by all partnership universities with respect to ethics and practice of information and data management on organisational levels are deficiencies in dissemination and

[22] Relevant provisions for the above considerations in the GDPR are: Articles 13 and 20 (EC 2016).
[23] Relevant provisions for the above considerations in the GDPR are: Articles 4(4), 9, 12, 13, 14, 15, 21, 22, 35(1) and (3) (EC 2016).

implementation of good data ethics conduct ("institution-wide quality culture of data ethics") and the practical incompleteness of institutional digitalised information and data systems (see Table 1). For example, the former may include inadequate consideration of ethical rules when responding to urgent requirements for the use of data under time pressure.

The case studies further show that three main opportunities exist that can be helpful for overcoming the identified weaknesses and avoid the threat(s): Improve on compliance with ECPDM and thus improve on compliance with GDPR; learn from national and international ethical codes of practice for data management; learn from national legislation on information and data management (see Table 1).

Table 1: Integrative SWOT analysis of ethics and practice of information and data management at the six partnership universities of the SQELT project (abbreviations[24] in brackets indicate which partner universities report the topic in question)

Strengths		**Weaknesses**	
1)	Compliance with GDPR and the national law that ensures GDPR enforcement (UA; BCU; UGhent; JU; DUK; UNIMI)	1)	Lack of an institutional Code of Ethics for Data Management (UA)
2)	Institutional digitalised information and data system (UA; BCU; UGhent; JU; DUK; UNIMI)	2)	Lack of an institutional Code of Conduct for Data Management (UA)
3)	Ethical principles of data management (UA; BCU; UGhent; JU; DUK; UNIMI)	3)	Lack of institutional policy of privacy and protection of personal data (UA)
4)	Code of Ethics/Code of Conduct/Ethical guidelines on data management at institutional level (BCU; UGhent; JU; UNIMI)	4)	Deficiencies in dissemination and implementation of good data ethics conduct (UA; BCU; UGhent; JU; DUK; UNIMI)
5)	Institutional Council of Ethics of Data Management (UA; BCU; UGhent)	5)	Incompleteness of institutional digitalised information and data system (UA; BCU; UGhent; JU; DUK; UNIMI)
6)	Data Protection Officer (UA; BCU; UGhent; JU; UNIMI)	6)	Lack of documents for data protection regulation that transfer the GDPR to specific L&T topics (UNIMI)
7)	Ethics codes/Codes of conduct/Ethical guidelines on data management in individual units (UA; UGhent)		
8)	Network of unit pivots for ethical data management (e.g. data collection coordinators) (UA; BCU; UGhent; JU; UNIMI)		
9)	Engagement of the Rectorate to improve on the ethics of institutional data management (UA; BCU; UGhent; JU)		
10)	Incorporation of the data ethics topic in the statutes (UA; UNIMI)		
Opportunities		**Threats**	
1)	Improve on compliance with ECPDM and thus improve on compliance with GDPR (UA; BCU; UGhent; JU; DUK; UNIMI)	1)	Possibility of hacker attacks to the university's digitalised information and data system (cyber-attacks and social engineering attacks)
2)	Learn from national and international ethical codes of practice for data management (e.g. research ethics) (UA; BCU; UGhent; JU; DUK; UNIMI)	2)	Unduly use of data that breaches the GDPR and this ECPDM
3)	Learn from national legislation on information and data management (UA; BCU; UGhent; JU; DUK; UNIMI)		

Beyond the weaknesses mentioned above the SQELT partnership universities see the following threats for ethics and practice of information and data management (in L&T): There is always the risk and real possibility of hacker attacks to the university's digitalised information and data system (e.g., cyber-attacks and social engineering attacks). Another omnipresent risk is the unduly use of data that breaches the GDPR and this ECPDM. This can typically happen because of unethical behaviour of some people who have access to

[24] UA = University of Aveiro; BCU = Birmingham City University; UGhent = Ghent University; DUK = Danube University Krems; UNIMI = University of Milan

data, that is because of misuse of data due to negligence or carelessness that could compromise confidentiality and anonymity of data including careless interaction and data exchange with other players in the field of (higher) education.

In general terms, the identified weaknesses and threats can be tackled (with a chance of success) by further developing the strengths mentioned in Table 1 and by improving the exploitation of the identified opportunities.[25]

[25] A more in-depth strategic SWOT analysis (Leiber et al., 2018, 352ff.) can possibly be made on another occasion.

APPENDIX 1: FROM THEORY TO PRACTICE – INSTITUTIONAL SQELT CASE STUDIES ABOUT DATA ETHICS IN LEARNING AND TEACHING

University of Aveiro

Basic aspects of data processing

The University of Aveiro (UAveiro) is fully responsible for personal data processing in compliance with the General Data Protection Regulations (GDPR) and the national law which ensures GDPR enforcement in Portugal.

The institution is also fully committed and engaged with protecting the privacy and personal data of its members and users in compliance with all principles and rules of data protection underpinning GDPR and the national legal enforcement, ensuring security and confidentiality.

The analysis of some internal documents shows which personal data are collected, for which purposes the institution may use them, how they are processed, with whom they can be shared, and for how long they are to be kept.

The institution's privacy policy covers the Information System of the University of Aveiro (SIUA) and is governed by the GDPR. The SIUA covers a wide range of data concerning all institutional users (staff and students) and a wide range of areas of activity (human resources, academic services, among others).

The University of Aveiro respects privacy of the information system's user, and ensures the security and confidentiality of all personal data that s/he needs to share with it using this system, and will not collect any personal information without the user's agreement under the terms required by the GDPR.

The data collected on SIUA forms will be used exclusively for processing user requests and will not be used for any other purpose, always protecting user confidentiality under the terms of the protection given in the above-mentioned regulations.

Processing of these data is the responsibility of the University of Aveiro and the data are stored in its information systems, which are properly protected. The information gathered can only be accessed and processed by members of the University of Aveiro in the course of their duties, with the purpose for which they have been collected always made clear in the respective documents collecting the data.

The University of Aveiro has a Data Protection Officer (DPO), who ensures compliance of the treatment of personal data with current legislation.

Regarding collection and use of technical information, the SIUA uses cookies, and the scope of its use of them is set out in the cookies policy.

Technical information is only held on our servers concerning visits to the SIUA, and information which could be used to identify visitors to the site is not collected. Technical information recorded is limited to the following:

- The IP (Internet Protocol) address of the visitor;
- The type of Internet browser used by the visitor to the site and the respective operating system used;
- The day and time of the consultation;
- The pages of the visited site and the downloaded documents. The technical information will only be used for statistical purposes.

Ethical principles of data management

In terms of ethics and ethical principles, the University of UAveiro has already in place some regulations, codes of conduct / practice in some of its units and services, and a dedicated committee – the Council of Ethics and Deontology. These achievements account already for the relevance that ethical issues have to

UAveiro. Nevertheless, there are still challenges to meet. UAveiro still lacks a general code of ethics / conduct for the entire institution, as for the time being only some of its units / services have one. This gap has been acknowledged by the present Rectory team, who has already engaged in covering it by addressing the issue and promote the work of drafting a Code of Ethics for the University of Aveiro.

In 2009, by the time UAveiro underwent a major institutional change that, among other things, promoted a governance change, the institution had the opportunity to create new governing bodies and decided then to create a Council of Ethics and Deontology. This Council is the advisory and support body for the governing boards in matters of ethics and deontology. Its aim is to promote reflection and contribute to the setting-up of appropriate directives for the establishment and consolidation of a policy of safeguarding ethical and deontological principles, in particular by issuing guidelines or proposing its own codes of conduct. Its regulation establishes:

- As privileged areas of action
  - ethics of the university performance regarding its internal and external members,
  - ethics of boards and actors' behaviour,
  - ethics of research protocols.
- Possibility of proposing codes of conduct for teachers, students, researchers, and doctoral students' supervisors.
- Taking decisions about the respect of norms and ethical principles in every area of the institution's scope of action.
- Full exemption and independence from the remaining boards of the university.

The Council of Ethics and Deontology is therefore the advisory board where all ethical issues are dealt with and where ethical principles are defined for the whole institution. It promotes, on a regular basis, public sessions where issues that concern ethics in general are presented and discussed, inviting for that purpose speakers with a leading reputation in the area. The existence of such a council is an achievement in terms of promoting good ethical principles and action at the institution. However, as we see it now, it needs to go further in terms of really implementing and disseminating among the academic community a good ethical conduct.

Further mention to codes of conduct and good practice is to be found in the university's statutes, namely addressing L&T aspects, good governance and management. All university members and boards have to abide by them.

Presently a draft proposal of a Code of Conduct for the entire university and a draft proposal of a "Doctoral School – Code of Practice" are underway.

The Information, Technology and Communication Services (STIC) also have a Code of Conduct for its Professionals in place since 2014. This document aims to set out what is an appropriate and valued behaviour in the exercise of these professionals' functions. It does not, however, address ethical aspects as such.

UAveiro has also in place an established network of DPO (Data Protection Officer) and GDPR pivots – one per unit/service. This team of GDPR pivots works together with the DPO, closely following all activities that involve personal data processing, from design to monitoring.

Moral and lawful bases for data management

GDPR and national legislation on data management had an impact on UAveiro. The institution had to prepare and adapt to it by implementing a set of actions:

- Collecting, analysing and registering ongoing processes relating to the normal functioning of the institution
- Collecting, analysing and registering all sources of information that have personal data
- Collecting, analysing and correcting technical conditions, both physical and organisational, of best safeguarding data, from collection, processing and filing

- Awareness-raising and involvement of the university's human structure
- Creation of an organisational model that ensures compliance with GDPR from conception onwards and by default.

The university has a DPO and a support team (a pivot per unit / service) prepared to help to build, follow and audit ongoing data management processes. Every time a new data management process is initiated there are a set of established actions to be followed:

- Prior risk analysis with respect to the rights and safeguard of the rights of privacy of potential data owners involved.
- Possible impact assessment.
- Registration and follow-up of all actions involving necessary personal data.

Informed consent is only one of the different possible ways of processing someone's personal data.

Considering the group of people working (teaching staff, researchers and non-teaching staff) and studying at UAveiro, the framework supporting data processing is mainly legal and contractual. It does not need a formal consent, rather information given to the users. This information concerning the data subject, when data is collected, is namely about:

- The purpose of data processing;
- The identification of the person in charge for data processing;
- Which personal data will be gathered and processed;
- Ways of collecting and processing personal data;
- Data storage period;
- Entities to which data might be communicated;
- The possibility of transferring data to third countries (outside the European Economic Area);
- The data subject rights and procedures for exercising them, namely the right of access, correction and erasure;
- The identification and contact of the Data Protection Officer;
- Any additional relevant information to ensure an equitable and transparent processing, considering the circumstances and the specific context in which personal data are to be treated.

When the university is requested to transfer data to other entities, such as governmental institutions and social security, there is legal legitimacy to send data over and explicit consent is not required. The need for an explicit consent applies only when the former situation does not apply: for example, when the academic community is asked to answer questionnaires about their own personal life.

At UAveiro informed consent is being applied to all new data processing, usually questionnaires. The intention is that it be applied to all cases. In the case of pictures in public events attended by a big number of people, making it impossible to have a written consent from all, a disclaimer is used, informing how the pictures taken will be used, and giving the chance for participants to be in a "dark area" where pictures will not be taken.

The University of Aveiro is still undergoing the process of registering all collected data and applying all further GDPR related obligations, such as erasing data that became unnecessary at some point and for which there is no legal obligation of keeping them (for example data related to students that had scholarship or accommodation at some point may no longer be necessary). In contrast, data such as the academic record on students enrolled at the University of Aveiro can never be erased.

Individual rights related to data management

Individual rights related to personal data management at the University of Aveiro are those established by GDPR. A policy of privacy and protection of personal data is currently under development and it is intended to address all staff, fellows and students of UAveiro.

According to the applicable data protection law, individuals may exercise their rights of access, rectification or erasure of their own personal data, the right to restrict processing, the right to object data processing and the right of data portability. In what concerns staff this can be done directly at Rhumo (a human resources portal) or through written request addressed to the Human Resources Services.

Therefore, the University of Aveiro must attend all requests from individuals in relation to the personal data concerning them that the institution has control on, must process, or transfer. The individuals have the right of access enabling them to verify the purpose of data processing, the categories of personal processed data, the recipients or categories of recipients who have access to their data; they have the right to know for how long the data is going to be kept, as well as the right to rectify them or erase them, among others. When personal data is subject to automatic processing and definition of profiles, UAveiro must provide information on the logic involved, as well as on the meaning and foreseeable consequences of this processing for the individual. GDPR adds that the individual should have the possibility to easily exercise this right at reasonable intervals, in order to know the data processing and verify its legality. It further suggests that the entity should use a secure system allowing individuals to access their personal data directly.

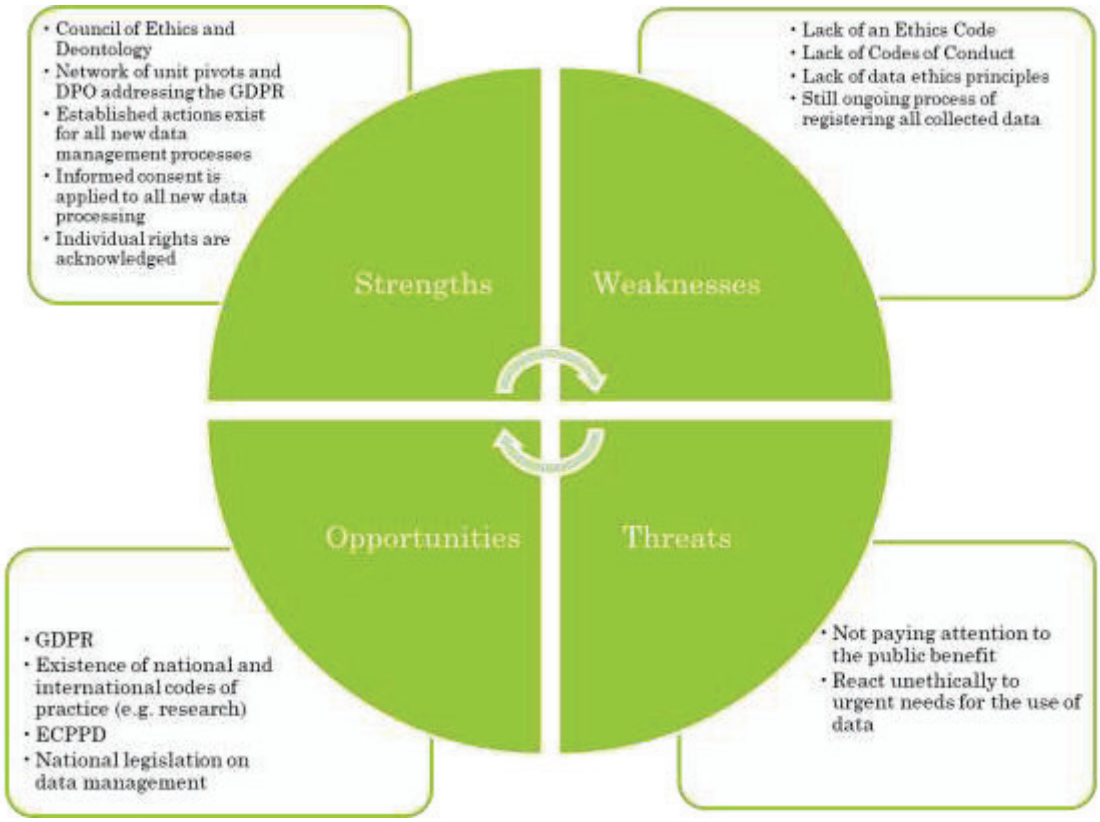
Final remarks

The analysis reveals that the University of Aveiro already achieved to implement most of the GDPR principles and is also already finalising a policy for privacy and protection of personal data. Overall, the university has already in place a network of DPO and GDPR pivots working together on a regular basis and widely disseminated throughout the academic community. Furthermore, the DPO work regarding GDPR full implementation at UAveiro is already impacting on the university's main processes and activities.

Nevertheless, the institution still faces some challenges regarding the actual implementation of a code of ethics and/or codes of conduct concerning the whole institution and specifically L&T.

A SWOT analysis of ethical principles, moral and lawful basis and individual rights related to data management at the University of Aveiro was done (Figure 1). It evidences what the university is already doing well, such as having a Council of Ethics and Deontology, responsible for all ethical issues at the university, a DPO and a network of GDPR pivots fully working, which allows for a good and widespread general knowledge about GDPR issues in the institution. It also shows the opportunities that can turn into advantages to the institution and become strengths, such as the GDPR in itself, national and international codes of practice that can help to frame the university's own code of ethics and practice, and even the Ethical Code of Practice for Performance Data (ECPDM), one of the outputs of the SQELT project. The analysis done to the university's current situation also evidences areas where the institution is not performing as well as it could: the institution still does not have its own code of ethics nor codes of conduct. And it also shows some threats these weaknesses expose the institution to, such as unethical behaviour in situations that need a quick reaction from the institution. That is, faced with an urgent request for some data, the university might not comply entirely with GDPR principles in the rush of responding to the request within the requested tight deadline, for example.

Figure 1: SWOT of ethical principles, moral and lawful basis and individual rights related to data management at the University of Aveiro (because of a recent conceptual change “ECPPD” in Figure 1 must be replaced by “ECPDM”)

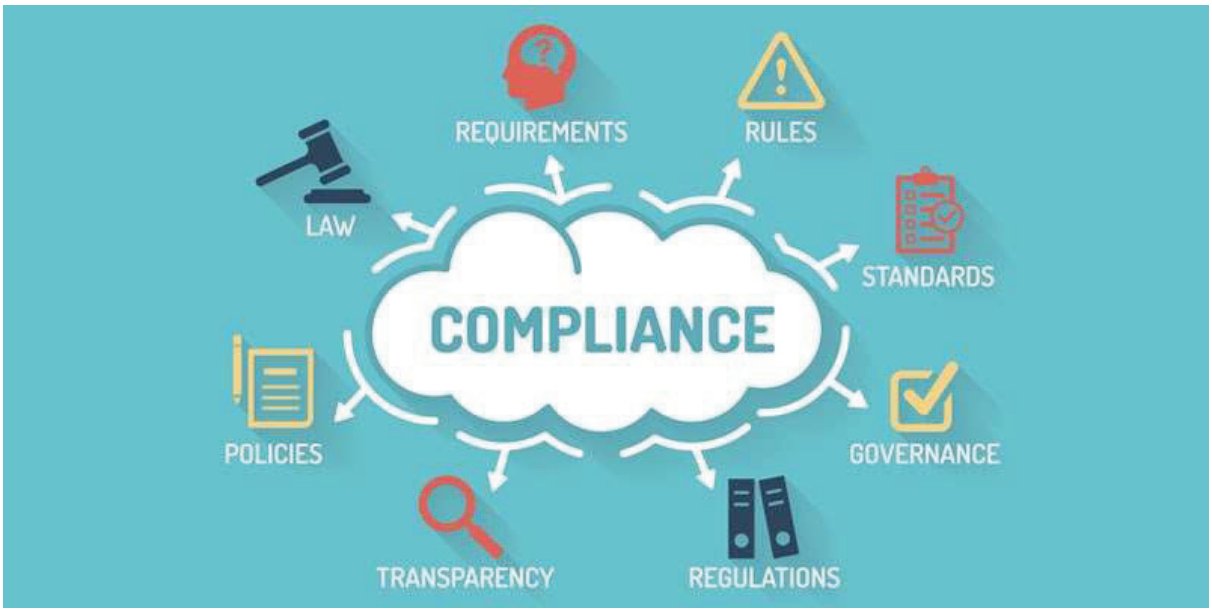


Birmingham City University

Guidance and rules for data management

Birmingham City University has a concise set of guidance and rules regarding data management. This is largely based on the current concern to ensure that the institution is GDPR compliant. The rules are primarily presented in a framework of compliance which relate to the requirements of the Law, to rules and regulations, standards, governance, policies and transparency. This can be seen in the University's own diagram relating to GDPR and data protection (see Figure 2).

Figure 2: Compliance at the heart of everything



However, the practice of learning analytics is governed by a range of ethical principles and beliefs about the use of data. As highlighted through interviews with colleagues, the practice of data collection and learning analytics is viewed as being about a commitment to the students and their well-being: the use of data is about improving the experience of the students. In particular, it is about developing an experience of the University that is tailored to their individual needs.

Data Protection

Regarding data protection, the University's intranet pages state that 'Birmingham City University is committed to safeguarding personal data, as a University we deal with a wealth of data and have a legal obligation to comply with Data Protection laws.' It is interesting that it then goes on to emphasise that data protection is a concern for all members of the institution: 'All members of the University dealing with personal data have a responsibility to familiarise themselves with BCU Data Protection Policies and the key principles of UK and EU Data Protection Laws.'

Freedom of Information Act (2000)

In addition to the GDPR, the University has a duty to abide by the Freedom of Information Act (2000), which came into force in 2005 and gives members of the public a right to see information held by public authorities. The Act was introduced to promote accountability and transparency in the public sector. BCU is considered to be a public authority under the terms of the Act.

Environmental Information Regulations

The University also has a duty to abide by the Environmental Information Regulations (2004), which 'provide public right of access' to environmental information held by public authorities. This includes information

about the University's activities relating to or affecting the environment such as land development, pollution levels, energy production, and waste management.

GDPR and the University

BCU guidance highlights that GDPR differs from the UK's Data Protection Act by introducing 'additional requirements for organisations who deal with personal data, managing compliance and providing evidence-based support to show compliance is key.' In particular, the University must now complete the Information Asset Register (IAR) as a 'fundamental component to provide the University with an overview of data processing activities and mitigate risks which may lead to non-compliance.' In addition, and perhaps of particular concern is that the 'financial penalties for non-compliance have been increased in addition to the reputational damage for the University.' BCU guidance also highlights that GDPR recognises technological advances in protecting data.

Ethical principles of data management

The seven ethical principles of data management outlined in the GDPR are present in the BCU guidelines.

1. Lawfulness, fairness and transparency

BCU guidance emphasises that data must be 'processed lawfully, fairly and transparently'.

> To ensure processing is fair we should have legitimate grounds for collecting and using personal data. Individuals should be informed that their data is being collected by BCU, what that data will be used for, and if it will be disclosed to any third parties.
>
> We must also make sure that we do not do anything with personal data that is illegal or would have an unjustified adverse effect on individuals.

2. Purpose limitation

BCU guidance emphasises that data must be 'collected for specified and legitimate purposes and not further used for other purposes'. The guidance highlights that 'this rule is amended where the further purpose involves research'

> This principle requires that we have a clear intended purpose, or purposes, for the personal data we collect and that we communicate the purpose(s) with the individuals concerned.
>
> We are required to notify the Information Commissioner's Office of the purposes for which we process personal data. Our current notification can be found in the Data Protection Register by searching for 'Birmingham City University'. If you intend to process personal data for any purpose not included in our current notification the notification must be updated, contact the Information Management team for assistance.

3. Data minimisation

BCU guidance emphasises that data must be 'adequate, relevant and limited to what is necessary.'

> This principle requires us to consider the purpose(s) for which we are collecting personal data for, before we collect it. By knowing what we need data for we are best placed to collect adequate and relevant personal data.
>
> This principle also guards against the collection of unnecessary data 'just in case' it may be useful in the future, as personal data should not be excessive to the purpose(s) it was collected for.
>
> For example, collecting the email addresses of students in order to contact them regarding a lecture series will be considered as relevant and adequate. But collecting their dates of birth for this purpose will be considered excessive.

4. Accuracy

BCU guidance emphasises that data must be ‘accurate and kept up to date.’

> This principle requires that we ensure the personal data we hold is accurate and up to date. The purpose for which the data are used will be relevant in deciding whether updating of the data is necessary, for example contact details will most probably need to be kept up to date as they serve no purpose if out of date. However, a change to a former student's name may need to be noted on their file, but it would be accurate to keep the name they had when awarded their degree on any copies of their degree certificate, rather than updating them.

5. Storage limitation

BCU guidance emphasises that data must only be ‘kept for as long as necessary for the purpose it was obtained for’. However, it highlights that ‘this rule is amended where the data is being used for research’.

> This principle requires us to keep personal data for the time necessary to achieve the purpose for which it was collected.
>
> Guidance on how long records should be kept for is available via our Records Management Pages. Records containing sensitive information such as personal data should always be disposed of securely.

BCU requires the following approach to storage of data:

> *Electronic*
>
> Staff should ensure sensitive information is stored securely using BCU’s approved systems only (i.e., OneDrive, Sharepoint, shared drive).
>
> Restricted access should be applied to ensure access is only available to staff who require the information to do their job.
>
> *Hard Copies / Paper Documents*
>
> If Confidential, mark on every page.
>
> If restricted, mark at least on front page or exterior surface.
>
> Store papers with sensitive information in a locked cabinet with access restricted on a need to know basis.

6. Integrity and confidentiality (security)

BCU guidance emphasises that data must be ‘processed in a manner ensuring appropriate security.’

> This principle requires that appropriate technical or organisational measures are taken by the University to protect personal data. This includes the protection of both physical (e.g. paper) or electronic information from risks such as unauthorised use/disclosure, accidental loss, destruction.
>
> All staff have the responsibility to ensure that personal data is kept securely, physically in locked cabinets or rooms as well as electronically in secure server locations or on encrypted external storage.
>
> Incidents where the University has failed to keep personal data secure should be reported for investigation.

At BCU, security is ensured by the following:

> Use OneDrive/Sharepoint where available and restrict permissions to allow access to the recipient only

Password protect/Encrypt documents and where possible contact the recipient by phone to provide the password

Disposal of data is covered by the following procedure:

Sensitive information must be securely disposed of and done so in accordance with the University's retention schedule.

7. Accountability/responsibility

The principle managers of data at BCU are the analysts in Planning and Performance. Their role is to collect data from all domains of the University to share internally with those staff who need it and externally with appropriate agencies such as HESA as part of national data reporting requirements. This group of staff are primarily concerned to ensure that data sharing does not breach GDPR and Data Protection laws.

However, in line with GDPR rules on accountability and responsibility, BCU has a group of 23 data collection co-ordinators across all the main domains of the University in addition to the team of three analysts in the Planning & Performance Department. The number of data collection co-ordinators in each domain varies. The role is usually performed by an 'executive PA' or other administrator but this is not universal. The co-ordinators in a number of domains (such as the International Office and Human Resources), are also heads of the department.

Moral and lawful bases for data management

At BCU, the six moral and lawful bases are covered in a range of ways.

1. Consent

BCU guidance highlights the focus of the new regulations on strengthening the rights of individuals and informed consent. A key element in this is giving individuals the right to choose 'what communications they receive and how they receive it.'

Key points:

1. Consent requires positive opt-in, we can no longer use pre-ticked boxes or any other method of default consent.
2. Consent must be explicit.
3. When requesting consent we must be specific, clear and concise.
4. Do not use a blanket approach to obtaining consent, if you are obtaining consent for separate things this must not be grouped together.
5. Make it clear how people can withdraw their consent – this should be an easy process
6. Keep evidence of consent, this should include who, when, how and what you told people
7. Consent should be reviewed as part of an ongoing process
8. Avoid making consent a precondition of a service.

2. Contract

The main concern is that data that is shared with external agencies as a reporting requirement is done so on the basis of data sharing agreements. Individual students are requested to sign an agreement with the University that their data may be used to satisfy the University's obligation to satisfy its legal obligations, vital interests, public task and legitimate interests.

BCU requires the following approach to sending data to third parties:

Prior to sending sensitive information to third parties, staff should ensure that the intended recipients are authorised to receive the information and that the measures adopted by the third parties provide adequate security for the confidentiality and integrity of the information being transferred, this should be in accordance with BCU's data protection policies.

3. Legal obligation

BCU is required to provide data to HESA and other national agencies regarding different aspects of higher education provision at the University. This includes the demography of students, employment of graduates and so-on.

Of particular interest and a cause of much controversy is the requirement to share data about students in cases relating to PREVENT, a government strategy that is focused on informing security agencies about students at risk of radicalisation and taking part in terrorist activity. All staff are required to undertake the e-learning module on PREVENT.

PREVENT is related to the wider issue of safeguarding vulnerable individuals and the duty of care. Data relating to individuals' vulnerabilities will be shared with appropriate authorities to ensure that students and staff are protected from bullying, violence and abuse.

4. Vital interests

The normal procedures at BCU take account of the need to share data when the data processing is necessary, for example, a medical emergency. An example from one UK university: 'A student collapses during a lecture and is unconscious. The lecturer calls for an ambulance and gives the paramedics the student's name and address.'

5. Public tasks

Data processing is undertaken at BCU to perform tasks in the public interest or for their official functions, and the task or function has a clear basis in law. In the case of BCU as at other universities, this covers activity such as:

- lecturing and tutoring;
- marking assignments and exams;
- awarding degrees;
- historic or scientific research.

The University Library, as with most others, has a distinct public task, under the Re-use of Public Sector Information Regulations, which is:

- to provide permission to use digital copies of images, manuscripts, documents, and objects in our collections for re-use in publications or through other media.

Of particular interest at BCU is that data collected relating to use of learning facilities, including the virtual learning environments and the library and learning resources are increasingly being used in an attempt to improve the individual learning experience and to tailor the individual experience of the University. This follows Sclater's (2016) ethical position that if an institution collects all this data, it should use it to improve the offer. Increasingly, too, the use of 'flipped' learning approaches, which rely on students using online material, such as viewing a lecture, to inform face-to-face classroom time involves engagement by staff with how students learn at home through analysis of data relating to VLE usage.

6. Legitimate interests

At BCU, as at most universities in the UK, legitimate interests include core business functions. The most commonly mentioned examples in documentation from a range of universities are 1) fraud prevention, which may include checking credit-card holders' details; and 2) activities around the graduation and relationships between the University and its alumni, where consent is not always possible or realistic.

Individual rights related to data management

The eight distinguishable rights for individuals with reference to the management of data related to them are covered by BCU in a range of ways:

The right to be informed

The individuals have the right to be informed about the collection and use of their personal data (GDPR key transparency requirement). BCU guidance observes that:

> It is important to note that sensitive personal data may only be processed when we have gained explicit consent, or the processing is strictly necessary, such as when information needs to be processed in an emergency or processing is required by law.

The right of data access

Individuals have the right to obtain access to, and copies of, the personal data that BCU holds about them.

The right to data rectification

Individuals have the right to request corrections to the personal data BCU holds if it is incorrect. More generally, this relates to the wider concern about accuracy of data. BCU guidance observes that:

> We are required to take reasonable steps to ensure the accuracy of the personal data we hold. Reasonable steps could include providing individuals with the opportunity to update inaccurate information we hold about them, such as providing students with the opportunity to review their record when enrolling.

The right to data erasure

Individuals have the right both to request that BCU ceases processing personal data and to request BCU to erase personal data.

The right to restrict data processing

Individuals have the right to request BCU to restrict data processing activities. BCU guidance suggests that,

> Where appropriate, individuals should be given the opportunity to 'opt out' of processing, however if there isn't a real choice an option should not be presented. For example if a student was given the choice to opt out of all processing when they sign up to a course, this would be a false choice as we need to process their data for the administration of their education. However it would be fair to allow them to opt out of other non-essential processing, such as receiving marketing communications.

The right to data portability

Individuals have the right to data portability of their personal data. At BCU, guidance observes that individuals have a right 'to receive a copy of the personal data BCU holds about the individual, in a reasonable format for the purpose of transmitting that personal data to another data controller.'

The right to object to data processing

BCU guidance notes that 'Individuals have the right to object, on grounds relating to an individual's particular situation, to any of BCU's particular processing activities where it has a disproportionate impact on the individual's rights.'

Rights in relation to automated decision-making and profiling

Individuals have rights related to automated decision-making based on their personal data including profiling. BCU guidance reflects that:

> If we intend to use or disclose personal data for any purpose that is additional or different to the purpose(s) it was originally collected for this use or disclosure must be something the individual would reasonably expect and should not have an unjustified adverse effect on them.
>
> We can inform individuals of the purposes their data will be processed for by issuing a privacy notice at the point data is collected. In cases where we are looking to re-purpose personal data we should where possible request consent to process the data for a new purpose or inform the individual(s) concerned.
>
> For example, the barriers at Millennium Point record the time at which staff and students enter or leave the building. This information is recorded for security purposes and for monitoring use of the building. It would not be fair or reasonable to re-purpose this information for monitoring staff timeliness without proper justification or informing those affected.

In addition, under Data Protection Laws individuals have the following rights:

- to require BCU not to send marketing communications;
- where processing is based on consent, an Individual may withdraw that consent, without affecting the lawfulness of the processing based on consent before its withdrawal.

Conclusion

It can be seen from the above that Birmingham City University, like most other universities, has developed its data protection rules, primarily driven by compliance needs. The need for strict procedures, at its most basic, is the concern of the University to avoid heavy financial penalties for breaching the regulations. However, it can also be argued that the basic principles outlined above and their practice at BCU reflects a deeper concern with working within an ethical code. The ethical code is based on the twin principles of informed consent for the individual from whom data is being collected and the notion that the purpose of data collection should be to improve the individual's experience of life at the University.

Ghent University

Data Management and the privacy issue

Over the years Ghent University has produced a series of documents, regulating the access to and the use of data. Gradually, and in compliance with legislation the focus has shifted from managing proper use of the system and data (from an ICT-point of view) towards privacy issues and ethical aspects.

Concerning data management in learning and teaching the student information system and the student learning management system are the main sources.

The new **student information system**, called OASIS (Education Administration and Student Information System) was implemented in 2010 and replaced an older database.

Since 2003 a **student learning management system** is being used. The first version, Minerva, was internally developed by the ICT Department in a Blackboard environment. Since 2019-20, a new student learning management system, Ufora (Brightspace) came into practice. It's providing a lot of statistics on students' behaviour in the system.

Here is an overview of the most important documents:

- Code of conduct for the use of Ghent University's study administration and student information (2013)
- List of Good practices containing questions for information/data from external parties and how to react (2014)
- A **vision on information security (2014)**
- Guidelines for the classification of information and data (2015)
- Working with personal data and confidential information in a secure manner (2015)
- Policy for correct usage of the UGent ICT infrastructure (2017)
- **Generic Code of Conduct** for the **processing of personal data and confidential information (2018)**

An internal website on information security contains all recent information.

The **vision on information security** (2014) was the first **cornerstone of Ghent University's Information Security Policy**. The strategic policy has been developed in accordance with national and international legislation, in particular privacy legislation. Best practices and (inter)national norms also have been taken into account. The vision strongly originated from the ICT point of view, from cyber security.

Its two-in-one approach combined:

  - **Privacy**: personal data are handled with care and thoroughly protected, in agreement with national and European legislation
  - **Cyber security**: information and information systems are sufficiently protected against intrusion and abuse
  - A substantial **overlap** between both

The three cornerstones in the information security were:

- **Integrity**: information used should be reliable and of good quality. It cannot (un)intentionally be changed wrongfully. Integrity also pertains to accuracy, completeness, correctness.
- **Confidentiality**: only authorized users have access to the correct information. Next to privacy protection confidentiality also includes exclusivity of information.
- **Availability**: information is readily available. It can be used at the request of an authorized user. An agreed level of service (concerning data and the electronic services) is guaranteed.

GDPR in Ghent University

To be fully compliant with the General Data Protection Regulation Ghent University issued the **Generic Code of Conduct for the processing of personal data and confidential information.**

The Code was adopted by the Executive Board on May 18, 2018. It is currently the central document in Ghent University's policy on data management; it puts forward regulations on the access and use of personal data and confidential data and provides for sanctions in case of violations. It applies to processing through IT-applications, but by extension also to manual processing of personal data and to the processing of confidential information at Ghent University.

The internal code of conduct pertains to all employees, students and, in case of collaboration, also to external partners.

The Generic Code of Conduct is a crucial element in the general data protection policy. To ensure the proper implementation a **Data Protection Officer** has been appointed. Her task is to coordinate and monitor the legitimate and secure processing of personal data at Ghent university.

A non-exhaustive overview of the categories of personal data processed by Ghent University is listed on the website https://www.ugent.be/en/ghentuniv/privacy/privacystatement.htm:

- 'Personal identification data: name; address; place of residence; place of birth; bank account number; telephone number; date of birth; gender; e-mail address
- Interaction data such as the IP address; cookies; surfing and clicking behaviour
- Images such as photos and videos
- Information about the study programme and training, such as decision-making on a course of study, study progress and study results
- Data collected in connection with scientific research'

Ghent University processes data for the following purposes:

- Educational matters
- Scientific research
- Personnel matters
- Business management operations

Future developments

The new student learning system (Brightspace) gave rise to a new debate on personal data and Learning Analytics. The detailed statistics on student behaviour in the programme alarmed the student representatives and they wrote a position on the issue, called 'Learning Analytics, monitoring and privacy'.

At the same time the **Royal Flemish Academy** wrote a **position, containing 16 recommendations on Learning Analytics**, in which data protection, privacy and ethics have a prominent role.

The discussion of the matter by the Educational Council resulted in **a workgroup**, which is in charge of writing **a code of conduct for Learning Analytics**. Benchmarking in foreign universities (esp. the Netherlands) was the first step in the process, which is still ongoing.

Parallel developments in the research domain

The Research Department has developed a policy framework on Research Data Management, which was approved by the Board of Governors on September 2, 2016. It is to be read in conjunction with the Ghent University Policy Plan on Research Integrity and the Ghent University Information Security Policy. The ethics of data management prove to be significant in research plans as well. A group of data stewards has been appointed to sensitize, advise and train researchers.

Ethical principles of data management

Ghent University's Generic Code of Conduct for the processing of personal data or confidential information states 7 principles from the GDPR to be complied with.

1. **Accountability:** Anyone who shares responsibility for the processing of personal data at Ghent University must demonstrate that **responsibility** has **actively** been taken to ensure that the processing takes place in a **lawful and secure** manner. A **record of processing activities** should document what personal data are processed and for what purposes. If the processing may involve a high risk, a description and assessment of the risks and foreseen measures will be demanded prior to the processing. If necessary, the Data Protection Officer must be consulted for advice.
2. **Confidentiality and integrity:** All users are required to treat the personal data and/or confidential information as confidential. Moreover, users have to take all reasonable steps to guarantee the confidentiality and integrity of the data processed. They have to make sure that the data are adequately protected in order to prevent unauthorised disclosure. The practical guidelines for working safely with IT resources and the information security policy of Ghent University can be consulted. All users are equally responsible for the integrity of the equipment used for processing (e.g. protection against damage, destruction, loss or theft). If a data leak (or other related incident) is detected, the Department of Information and Communication Technology, which is the central contact point for this purpose, must be informed straight away.
3. **Lawfulness, fairness and transparency:** All processing of personal data and or/confidential data shall be in compliance with all applicable laws, regulations and rules. The users shall show the necessary ethical integrity during this process. The fact that the user collects, uses, consults or otherwise processes the data shall be clear to the hierarchical line and to the data subjects.
4. **Purpose limitation (finality and proportionality):** The purposes for which the data are processed must be clearly defined and documented for each application. All users shall respect the specific purposes and processing shall be proportionate to the purpose. Any additional and therefore improper use of the data is not permitted. Users are given access on a need-to-know basis, if possible, this can be enforced technically. Additional processing can be exceptionally permitted within the context of the specific legislation or regulations (e.g. scientific or historical research or statistical purposes, for archiving in the public interest, or for further research of control mechanisms for scientific integrity).
5. **Data minimisation:** Users cannot process (e.g. consult, collect) more data than necessary for the defined purposes. The processing of personal data is restricted to situations where the purpose cannot be achieved by other means. The use of anonymised data is the rule. Pseudonymised (also referred as 'coded') personal data shall be used if the intended purpose cannot be achieved by using anonymous data. Only a detailed justification of the fact that the intended purpose cannot be achieved by means of anonymised or pseudonymised data allows the processing of raw personal data.
6. **Accuracy:** Users shall ensure that the data they process is correct and up to date. All reasonable steps shall be taken to ensure that inaccurate data is corrected, either on the initiative of the user or at the request of data subjects. The data subjects will be informed of this option by means of an informed consent form or an online privacy notice.
7. **Storage limitation:** The storage period/retention of personal data and confidential information is in accordance with all relevant legal provisions and applicable agreements. Users have to limit the storage period/retention period to what is necessary and in accordance with the original purposes. Longer retention can exceptionally be allowed if it is within the context of the legislation or regulations established for this purpose (e.g. for scientific or historical research or statistical purposes, for archiving in the public interest, or for further research or control mechanisms for scientific integrity). After the expiration of the retention period, the users will have to completely and securely delete the data, according to the guidelines in the information security policy of Ghent University.

Moral and lawful bases for data management

The legal framework for the processing of personal data and confidential information is determined by:

- the General Data Protection Regulation (GDPR). Cf. above. This European privacy regulation is directly applicable as of 25 May 2018, without prior transposition into national law.
- Belgian privacy legislation, in particular the Law of 8 December 1992 on the protection of privacy with regard to the processing of personal data, together with all amendments and implementing decrees.

Individual rights related to data management

The Ghent University privacy statement mentions the rights of the data subject with regard to the processing of personal data. https://www.ugent.be/en/ghentuniv/privacy/privacystatement.htm

These following rights are drawn from the GDPR:

- 'The right to request which personal data are processed and, if such data are not provided directly to Ghent University, to request information concerning the source of such data;
- The right to request the rectification of incorrect data;
- The right to request 'to be forgotten (right to erasure)', provided a number of conditions are met;
- The right to request the provision of certain data in order that the data subject may transfer the same to another organisation;
- The right to object to the processing of personal data through fully automated processing (e.g. direct marketing).'

A data subject can exercise its rights as follows.

If students or personnel have any questions about the rights and obligations concerning privacy, or if they think that Ghent University is processing their personal data in a wrong and/or improper way, they can **contact the Data Protection Officer**.

At the level of Flemish higher education there's a **Flemish Supervisory Committee for the processing of personal data**. People who aren't satisfied with the way the university treated their request or complaint can contact the Flemish supervisor.

Conclusion

Ghent University has incorporated the GDPR in its own regulations through the Generic Code of Conduct for the processing of personal data and confidential information. A Data Protection Officer has been appointed to coordinate and monitor the legitimate and secure processing of personal data and the implementation of the Generic Code of Conduct. The issue of ethics in data management remains high on the agenda, as can be illustrated by the workgroup on a Code of Conduct for (the use of data in) Learning Analytics.

Strengths

- Good basis: texts and regulations are present, especially the Generic Code of Conduct
- Link with cybersecurity
- Awareness of the issue in a wide range of staff and students
- Discussions and follow-up in the appropriate fora (Educational Council, …)

Weaknesses

- Information and responsibility are dispersed (different departments, ICT, Education Policy, Administrative Affairs, Research) and cooperation across departments can be improved.
- Limited transparency, not all staff is aware of the existing documents and commitments

- A Communication strategy needs to be developed.
- The responsibility of controlling for violations of rules is not thoroughly defined.

Opportunities

- The workgroup and the future code of conduct for the learning management system can be a catalysator for more cooperation over departments.
- A communication strategy can be improved and concerted over departments.
- The position of the Royal Flemish Academy and an interuniversity workgroup can enhance cooperation on the matter, both between and inside universities.
- The Data Protection Officer has an overview of all actions and regulations and can set new initiatives in motion.

Threats

- Corporate culture and limited time frames may prevent adequate and lasting cooperation.
- The startup of the new learning management system for 40,000 students and over 1,500 teaching staff has been facing some hurdles; insufficient training may lead to unforeseen consequences/ inadequate data handling, ….

Jagiellonian University in Kraków

Pursuant to Polish data protection regulations [the Polish Data Protection Act of 10 May 2018], the Jagiellonian University in Krakow, like other institutions in Poland, is obliged to implement the principles of data processing set out in the GDPR. In this context, their use cannot therefore be considered as an achievement but as compliance with applicable law. The correctness of data processing is supervised and monitored by the JU Data Protection Officer. The main source of challenges in applying both the Polish and the EU law lies in the complexity and instability of Polish regulations and policies, which tend to change too often.

Ethical principles of data management

The following principles of data management have been defined at JU:

- Lawfulness, fairness and transparency: the personal data administrator, incorporated into the central institutional system of JU, fulfilling the role and responsibilities as described in the Polish Data Protection Act bill, is obliged to provide access to personal data to the data subject. This obligation is respected, although the challenge is access to documents archived by law, especially outside IT systems.
- Purpose of limitation and Data minimisation: most university data is collected only for legitimate purposes, although the legal definitions of these purposes change much more often than the purposes themselves (e.g., the new model of doctoral studies in Poland, the personal data of candidates who resigned from study before the 1st October, the legal status of contact data of graduates). The other type of data, like statistical reports or study program documentation, should correspond with current needs, however it is difficult to put such demands on scientists who are trying to explore new solutions for existing problems.
- Accuracy: personal data that can be easily verified is not a challenge, while aggregate data processed for reporting purposes is more problematic due to the changing definitions of indicators that hinder comparisons over the years.
- Storage limitation: personal data, the archiving of which is not required by law, are deleted or anonymized, although there is a risk posed by the human factor because the demarcation of necessary and additional documents is not always obvious.
- Integrity and confidentiality: data security procedures include both ICT and physical security.
- Accountability/responsibility: the way of implementing the provisions is specified in internal documents and supervised by the Data Protection Officer.

Moral and lawful bases for data management

Most of the personal data at the JU is collected for legal purposes and public tasks related to documenting the education process (e.g. study history, students' achievements), employee matters (e.g. work history, salaries) as well as accounting and settlements (e.g. bank accounts, job contracts). Some of them, such as additional forms of education offered by the university, require separate contracts. In addition, there are areas requiring voluntary consent, such as additional scientific, cultural or sports offers, or support for students with disabilities. The main challenge for universities is to correctly distinguish these areas, which is the subject of constant discussion also at ministerial level.

Individual rights related to data management

According to the law, every data subject has the right to be informed, to have data access, rectification, erasure and portability, to restrict and object data processing. Procedures for dealing with such requests are included in the rector's ordinances. Restrictions on these rights are based on overriding purposes because a public university is required to store and archive much data, which is in accordance with GDPR and ECPDM. Any disputes may be settled by a court.

Danube University Krems

Ethical principles of data management

Danube University Krems (DUK) represents a type of higher education institution (HEI), which is a university (and not another type of a HEI), by this defining DUK as one of the member universities of the cluster of public universities in Austria (which are dominating the Austrian higher education system). Even though DUK represents some features that clearly resemble features of universities of applied arts, the one interpretation is that DUK is focusing and re-inventing application-oriented teaching features (with some association of third mission activities) within the organisational frame of a university. Concerning its functional profile, DUK emphasizes (traditionally speaking) the teaching and education aspects, and here again placing a particular focus on continuing education. With regard to research, DUK crafted the understanding also of a "teaching-based research". In reference to data management, it appears necessary to distinguish between the "external" and "internal" data management (systems).

External data management of the Austrian higher education system:

Currently, Austria has twenty-two public universities. They are all subject to the same governance (policy) system that defines the relationship between the universities and the responsible federal ministry, which is now being called the "Bundesministerium für Bildung, Wissenschaft und Forschung" (BMBWF, Federal Ministry of Education, Science and Research). The BMBWF is the prime public (and by this overall) funder of 99 public universities in Austria. Universities are obliged to develop so-called Development Plans ("Entwicklungsplan"), valid for six years, but being adapted in-between. These Development Plans are the basis for the so-called three-year Performance Agreements ("Leistungsvereinbarungen"), between the concrete university and the federal ministry (BMBWF), which then again are being supported by an annual reporting over a whole spectrum of indicators (also in reference to teaching, but also other areas), which every university must submit to the federal university each year. This indicator reporting is being called Intellectual Capital Reports ("Wissensbillanzen"). A few of these indicators on teaching clearly qualify as "performance indicators". In that sense, and formulated as a hypothesis, the focus of these indicators is more so on teaching, and less so on learning. These cycles of Development Plans, Performance Agreements and Intellectual Capital Reports are repetitive.

There is an interest in a maximum transparency, concerning the public accessibility of the documents in relation to the public governance cycles of the public universities, and also of the Intellectual Capital Reports ("Wissensbilanzen"). So all the documents with regard to public governance cycles can be accessed on the internet (https://unidata.gv.at/Pages/default.aspx). This also includes the individual annual indicator reporting of all universities, which are being submitted via the annual Intellectual Capital Reports. In addition, on an aggregated (and by this anonymized) basis, every interested user can access these indicators for the purpose of an analysis (https://unidata.gv.at/Pages/auswertungen.aspx); also focusing more specifically on teaching and learning (https://unidata.gv.at/Pages/auswertungen.aspx). In that sense, a whole spectrum of performance indicators on the Austrian public universities is publicly accessible in Austria, for sure for teaching, and to a lesser extent also for learning (depending on how learning is being defined).

Therefore, with regard to this external data management, we can consider the following ethical principles:

- In reference to a preselected number of indicators (across the whole functional profile of a university, covering teaching and research, but also other areas), every public university, on an annual basis and in reference to agreed-upon deadlines, must report these indicators to the respective federal ministry (now called BMBWF). With a few exceptions (for example, publications), these indicators are aggregated, and do not allow person-specific conclusions.
- The ministry is implementing the reported indicators into ministry-internal data bases.
- As a part of the annual Intellectual Capital Reports ("Wissensbilanzen"), every university produces an annual report on indicator performance, which is published on a public website (maintained by the ministry), and which can be accessed by everyone and from everywhere (across the world).These indicators are aggregated to the institutional level.

- The ministry allows open-access to specific segments of the ministry-internal data base, which is based on the (by the universities) reported indicators. In this open access mode, not all indicators can be approached, and it is not possible to track back the indicators to the individual universities.
- Put in summary, the core ethical principle is transparency, emphasizing the aggregated compilation of the indicators, which should provide rationally generated information, which may inform decision-making with the quality of a fairness.

Internal data management of the Danube University Krems (DUK):

The focus of DUK is on education, more so on continuing education. Organisational principles of DUK concentrate on study programs ("Lehrgänge"), so these study programs are driving the whole organisation in terms of structuring the organisation, and are defining teaching and education (and learning) as core activities. Research and third-mission activities (innovation) ought to refer (in one way or another) to the teaching focus of DUK. Continuing education is the other organisational principle that is structuring DUK, with several implications and ramifications. Teaching content and learning interests express this continuing-education orientation. Students at DUK often are demonstrating particular characteristics (when compared with students at the other public universities in Austria), such as being older, having already prior occupational (professional) work experience, are showing a more clearly articulated career interest, and are frequently obliged to pay tuition fees.

At DUK, a complex set of tools already exists, referring to teaching and learning performance indicators. Every course must be evaluated. Typically, the teachers and the program heads are receiving this information about the results of the teaching evaluation (automatically). One aggregation level higher, graduates are normally being asked, one year after graduation, to provide an assessment of their completed study-programs, in context of the so-called Study Program Final Evaluation. In addition, all the study programs are also being documented (annually) by different statistical figures, for example referring to the number of students, the number of beginning students and the number of students taking longer than the designed time. Public accessibility to this diversified information on teaching (teaching and learning) is normally not the case.

Furthermore, DUK also engages in peer review and quality enhancement: Quality enhancement for sure marks an area, where there is learning in place. Peer reviews are not so much interested in measuring performance. Performance indicators support peer review, but peer review is more than being primarily based on performance indicators. Teaching and Learning, most commonly, will be (will be also) on the agenda of a peer review exercise (at least in the one or other form). In the understanding of the Danube University Krems, peer review and quality enhancement are connected with the internal governance system of the university.

Therefore, with regard to this internal data management, we can consider the following ethical principles:

- Students are being regarded as the primary group (of stake holders), whose interests, objectives and concerns must be addressed (we want to put this here at least as a proposition). Carrying this argument further, structures and processes of the whole organization of the DUK are to be set up in a way, so to reflect this vision and mission.
- Students at DUK engage primarily in continuing education. In that sense, the circumstances and interests of these students are to be reflected in a particular way.
- Teachers of the specific courses, but also the heads of the study programs, are to be expected to support in various ways the students in their continuing-education efforts at DUK.
- One of the most important ethical principles here is fairness. Fairness for the students means that teaching (and education and learning) at DUK are to be so designed and so practised that this is a teaching in accordance with principles of continuing education. Fairness for the teachers, heads of study programs and other faculty members means that all performance monitoring measures (for example, the evaluation of the specific) courses always is being accompanied by reflections (for example, talks between teachers and heads of programs in case of course evaluation), so to allow

for broader assessments, and to inquire on possibilities and options for improvement (but again clearly in fair ways).

Moral and lawful bases for data management

The internal data management at Danube University Krems (DUK) is in full accordance with the law. The internal data management at DUK is therefore law-based. This is being regarded as a moral obligation of DUK. DUK fully supports the basic right of data protection ("Grundrecht auf Datenschutz"). There are two main legal sources for data protection in Austria: the DSG ("Österreichisches Datenschutzgesetz", Austrian data protection law), and the more recently released General Data Protection Regulation (GDPR) of the EU, which came into effect on May 25, 2018 (called in German: "EU Datenschutz-Grundverordnung", DSGVO). The DSGVO represent the historical legal pattern, to which data management at DUK refers (referred) to, while the GDPR clearly has implied that data protection at DUK is in a process of transformation to new and higher standards.

The Austrian data protection law, DSG ("Österreichisches Datenschutzgesetz"):

From this basic right of data protection it follows that every person, particularly in reference to her or his private and family life, is entitled that confidentiality is being applied to her or his personal data, especially if this represents a legitimate interest of the person. One implication of this is that all employees of DUK have signed a clause on confidentiality in their employment contracts (or also other types of contracts, being it, for example, teaching contracts or free-lance-arrangement), which they are being expected to apply in all of their DUK work activities. In order to implement the regulations created in DSG, specifically for the protection of data secrecy in work relationships, the employees have also signed the corresponding declarations of commitment, which are managed by the DUK administration ("Dienstleistungseinrichtung [DLE] Personal", the staff service unit).

The EU General Data Protection Regulation, GDPR ("EU Datenschutz Grundverordnung", DSGVO):

There is a general consensus that the GDPR has led to a considerable increase of data protection and data protection regulations. The one implication is that the GDPR is interpreting the rights in association with data protection to a greater extent. Complementarily, GDPR also has (and is continuously further developing) a greater sensitivity for the use of data, and by this for data management generally in the broader contexts of practice and application. There are several ramifications for data management at DUK:

- While it may be said that DSGO is focusing on the creation, better the lawful creation of data, this of course is also true for the GDPR. However, GDPR is referring more widely also on the use of data, and by this the data management from a practical perspective. GDPR looks on the "dynamic" aspects of data management.
- DUK had to re-evaluate its data management, prior under DSG, in terms of whether this still fully meets the new requirements under GDPR. Commonly it is being said that GDPR is carrying data protection to new and higher levels of quality standards for data protection and data management.
- GDPR has required the DUK to expose its systems and its structures and processes (routines) of data management to permanent reflection and assessment, in the sense of: What (which data) are being created and stored by the university? (Which data does the university "have", all together?) Who can access the data? What is the purpose of the data? Is the purpose still valid, or, if purposes alter, what does this mean for the continued storage of data or the creation of new data? Finally, do data have a lifetime, meaning that there is an obligation to also erase data, and if so, when?
- GDPR had (and has) the one concrete consequence that there is now more data protection particularly for the data of students at DUK, to ensure that student data are being used in sensitive ways. For example, this refers to how or how often interested (prospective future) students can be contacted by DUK. There is also the guideline of contacting students through the e-mail accounts that students have registered formally themselves with DUK university.

- The overall bottom line here is that GDPR has impacted and altered the governance (governance system) of data management of DUK in considerable ways.

DUK also has the official position of a Data Protection Officer ("Datenschutzbeauftragte/r"), who, in the current organigram of the university, is assigned as a person to the Vice-Rectorate of Teaching and Continuing Education in the Sciences ("Vizerektorat für Lehre / Wissenschaftliche Weiterbildung").

As a general policy, DUK is informing (public access) on its institutional website about its policies on data protection (https://www.donau-uni.ac.at/de/universitaet/datenschutz.html).

Individual rights related to data management

The core principle and understanding is that every member of the Danube University Krems (DUK) community (the students, but also the faculty and the administration) is to be informed, which data about them have been created by the university, which data are being stored (how) and for which purpose (purposes). The whole data management of DUK is law-based and is in full accordance with the law (national law and EU law). The organization of DUK also has (and develops further) the structures and processes, so that the law-grounding of its data management also can be performed and applied in good practice.

Reflecting on the current situation, the following can be said about the individual rights related to data management at DUK:

- Every individual person is explicitly to be informed should individual data about her or him be created or stored in the data management system of the university. The individual person also is always to be informed about the purpose (purposes) of any data creation or data storage.
- Every individual person has the right (entitlement) to correct (adapt, update) data about her or him.
- Every individual person has the right (entitlement) that data about her or him can (under certain circumstances) be erased or cancelled in the data management system, if there are not exemptions to this, being stated by the GDPR (EU General Data Protection Regulation).
- Every individual person has the right (entitlement) to formulate inputs in relation to the processing and application of his or her data, to which the university must reply.
- Every individual person has the right (entitlement) that her or his individual interests cannot become subject to automated routines of decision-making (in the sense of a "profiling").

Consequently, every individual person from the DUK community is entitled to pose questions or inquiries about the data management, about her or him, to the Data Protection Officer ("Datenschutzbeauftragte/r") at DUK (via the e-mail account datenschutz@donau-uni.ac.at), who has to respond within one month.

It is evident that any system of data management (or any governance thereof), also in relation to performance indicators, must take these legal regulations into account and must fulfil them. DUK is operating in this context.

University of Milan

UNIMI presents a set of guidelines which regulates all the procedures related to data management in general and a restricted set explicitly on all the data about students and the L&T process.

The former stem directly from the law n. 196/2003 and the European General Data Protection Regulation (EC 2016) and consist of two main documents: the "*privacy code*" and the "*guidelines on the treatment of sensitive data*", which display a specific schedule concerning data on students' enrolment and career. These documents define what a sensitive data is, the individual and duties rights related to data management, and the rules that govern the management and treatment of the data.

The latter regard two specific areas of the L&T domain, namely the student's survey and the use of the Learning Management System (LMS) from both students and teachers. Concerning the students' survey, UNIMI approved in September 2018 a specific policy on the processes of collection, elaboration, use and communication of students' opinion on teaching activities which are collected online at the end of each course (QAC, 2018). The policy has been developed and proposed to the Senate by the Quality Assurance Committee (QAC), that is the body in charge of coordinating the internal quality assurance process and in particular the students' survey. Regarding digital education tools, UNIMI has written specific conditions on use of the services for all the stakeholders using the LMS.

Ethical principles of data management

All the seven above-mentioned ethical principles of data management illustrated in the European General Data Protection Regulation (EC 2016) can be clearly identified within the above-mentioned UNIMI's regulations too. The principles of "Lawfulness", "Data minimisation", "Accuracy" and "Storage limitation" can be easily be retrieved from the article 8 of UNIMI's "*privacy code*" which describes the principles that rule the data collection process (article 8 pag. 8). In particular, it states that personal data has to be:

- Treated in a lawful and correct manner (*principle of "Lawfulness"*)
- Collected and recorded for specific, explicit and legitimate purposes
- Accurate and, if necessary, updated (*principle of "Accuracy"*)
- Relevant, complete and not excessive in relation to the purposes for which they were collected and subsequently processed (*principle of "Data minimisation"*)
- Stored in a form that allows identification of individuals for a period of time not longer than that necessary for the purposes for which the data were collected or subsequently processed (*principle of "Storage limitation"*)

The principle of "*Purpose limitation*" is clearly identifiable in the UNIMI's "*privacy code*" (article 3, p. 4). It is underlined that any request for access to personal data by the structures, bodies and individuals must be duly justified and connected with the execution of the activity that each subject has to carry out. Moreover, the request will be considered in the necessary but not excessive extent to the pursuit of institutional interest.

The principle of "*integrity and confidentiality*" is expressed in article 17 of the "*privacy code*" (p. 15-16) that argues how for personal and sensitive data that are stored and treated by automatized means is necessary to use encryption techniques or identification codes that allow to trace the individual – only in an extreme case of need. The University organizes all the procedures that are needed to obtain the above-mentioned result. Consequently, the informative systems are set up to minimize the use of personal data with identification when the same institutional purpose can be achieved through the treatment of data that have been anonymized.

Finally, concerning the "*accountability/responsibility*" principle, UNIMI presents its own data protection officer and displays reviews of the data management guidelines over time.

UNIMI has also adopted a specific policy on the processes of collection, elaboration, use and communication of students' opinion, as aforementioned. It is clearly aligned with the ethical principles here illustrated and the successive individuals rights; it also prescribes specific conditions related to communication of students' opinions in order to reduce the previous high internal heterogeneity concerning the public diffusion of the result of students' survey. These guidelines are based on two principles:

- Publicity of the results as an element of transparency towards students and society;
- Importance of the respect of teachers' privacy in relation also to academics' autonomy and freedom.

In order to balance transparency and public access of students' survey results, this document identifies all the subjects/bodies that can freely access the data and in which form (the name of the course/teacher is anonymized or not). A teacher can still decide to diffuse the students survey results of his/her course, but this is up to the individual choice of each teacher. Only the President of the teaching committee, the members of the Commission Students-Teachers and the Head of Department can see the results of the student survey in a complete transparent (non-anonymized) form.

Finally, this policy also provides some 'good practices' and principles to be followed for each stakeholder involved (mainly teachers and students but not exclusively) concerning their role in relation to an effective and transparent implementation of the students survey. So, for example, it is recommends that each teacher should illustrate the survey results of the previous year at the beginning of the course, illustrating the improvement actions undertaken on the basis of students' opinions and comment with students the answers to the open questions of the survey (about suggestions and criticism) before the end of the course.

Similarly, students are suggested to fill the survey after 2/3 of the course and not just before the enrolment for the final exam (the student survey is compulsory to do the final exam), in order to not loose memories about the learning experience.

Lastly, the President of the teaching committee of each degree programme should consider the following risks during the analysis of the results of the student survey:

- the negative exposure of either demanding teachers or more demanding disciplines;
- the excessive positive evaluation for basic and less demanding courses;
- the discouragement of a high-quality teaching and need for students' commitment.

Moral and lawful bases for data management

Some of the "moral and lawful" bases for the processing of personal data can be identified in UNIMI's regulation on this topic. The consent and contract are certainly present in UNIMI's policies. Regarding the consent, students give a general agreement on the collection and use of data at the moment of their enrolment. These mainly relate to their career progression as well as personal information like gender, age and all the information concerning previous studies. Secondly, the contract base is used as well for data management within UNIMI. Data on employment or further studies of graduates are collected by 'Alma Laurea', which is an Inter-University Consortium that manages the collection and storage of these types of data. Certainly, also legal obligation drives data management in UNIMI. The internal quality assurance process (described in the Intellectual Output O1, Benchlearning Report) prescribes the collection and use of specific data on the L&T process. These internal processes are thus compulsory in order to comply with the legislation on quality assurance (legislative decree n.19 of 2012 and the ministerial decree n. 987 of 2016).

Individual rights related to data management

The UNIMI "*privacy code*" identifies five individual rights that are mainly consistent with those reported in Chapter 2 of the European General Data Protection Regulation (EC 2016). Besides the individual's rights, the "privacy code" also defines the ways through which claiming and enforcing these rights is possible. These are reported as follows:

1) To obtain the confirmation (proof) of the existence of personal data and the access to them;

2) To obtain an explanation concerning the source of the data, the logic applied to the electronic treatment, the identification details of the owner and the person in charge of the data treatment, the categories of actors to whom the data can be communicated or that can know the data based on their responsibility/administrative position;

3) To obtain the updating, amendment, deletion, block or transformation in anonymized form of the data treated in violation of the law, including those whose conservation is not necessary in relation to the purposes based on which they have been collected and treated.

4) To obtain proofs that the previous actions (at point 2) have been carried out;

5) To oppose wholly or partially and according to legitimated reasons, to the treatment of personal data if these are used for marketing and commercial reasons.

Moreover, the guideline on the use of services of the LMS highlights further rights/duties for the stakeholders involved which mainly regard the type of contents that can be shared through the online platform (Ariel). In particular, the two following points are relevant in relation to data ethics in L&T:

- The teaching materials available on the LMS must be used only for learning purposes without harming the property rights on the authors of the materials. The free reproduction, diffusion and distribution of any materials is forbidden without a prior authorization released by the University.

- Each stakeholder must assume a correct and appropriate behaviour in relation to the uploading, management and diffusion of the materials within the LMS. In particular, it is underlined that a stakeholder must not use expressions aimed to directly or indirectly denigrate any other physical or juridical person and that it is forbidden to publish material offensive to public decorum or more in general that does not concern the object of study. The University can then remove any materials that is judged to violate the above-mentioned rules, according to its discretion and unquestionable judgment.

References

- Università degli studi di Milano (UNIMI) 2016. "*Regolamento di attuazione del d.lgs 196/2003 (codice privacy) recante norme in materia di protezione dei dati personali*". UNIMI: Milan.

- Presidio di Quality (QAC) 2018. "*Policy di Ateneo per la rilevazione, elaborazione, utilizzo e comunicazione delle opinioni degli studenti sulla didattica*", UNIMI: Milan.

APPENDIX 2: PROJECT WORKBOOK FRAMEWORK ON DATA ETHICS

This Appendix contains a Project Workbook Framework on Data Ethics (PWFDE) which is meant to complement the Ethical Code of Practice for Data Management (ECPDM). The PWFDE is inspired by the "Data Ethics Workbook" of the UK's Department for Digital, Culture, Media and Sport (DDCMS 2018) but it differs significantly from it.

The present PWFDE explicitly refers to ECPDM and provides a framework for ethics of data management to be offered to and applied by projects that comprise (personal) data protection issues. Following two broad principles of data handling ethics, the PWFDE asks questions to such projects, the answers to which help optimise the project regarding data protection or to revise the project if necessary. In this sense, the PWFDE can be used as an improvement-oriented evaluation tool for a project's alignment with GDPR and ECPDM. Particularly, the PWFDE should be used to consider ethical and legal questions to inform the best use of data. The PWFDE is designed to be regularly revisited throughout a project's lifetime, particularly in the planning phase and at the beginning of the project and when any changes are made to the data collection, interpretation, analysis, dissemination and storage.

The two principles of data handling ethics, that constitute the PWFDE, are:

- Clarify the project goals that are oriented at user need and stakeholders' benefit
- Obey the relevant legislation, ethical rules and codes of practice

These two principles are outlined in Table 3 along with the associated tasks to be solved and questions to answered by teams planning to undertake a project that involves (personal) privacy issues. Table 3 also mentions related Lickert scales for the assessment of the tasks which can be oriented at various guiding questions, without being limited to them, that are also depicted in Table 3.

Table 3: Project Workbook Framework on Data Ethics (PWFDE)

PRINCIPLES OF DATA HANDLING ETHICS AND ASSOCIATED TASKS	**LICKERT SCALE FOR THE ASSESSMENT OF TASKS**					
	0	1	2	3	4	5
1. Clarify the project goals that are oriented at user need and stakeholders' benefit	Project goals are not well defined					Project goals are clearly defined
Describe the project goals with supporting evidence.						
Orienting questions: How do the project goals benefit various users and stakeholders and clients? How is it achieved that everyone in the project team understands the project goals?						
2. Obey the relevant legislation, ethical rules and codes of practice	Obeyance of relevant legislation, ethical rules and codes of practice is not given					Obeyance of relevant legislation, ethical rules and codes of practice is well given
Obey the pieces of legislation, ethical guidance and codes of practice that apply to the project.						
Orienting questions: How is it achieved that evidence is given that all Ethical Principles of Data Management, Moral and Lawful Bases for Data Management and Individual Rights related to Data Management of the above ECPDM are respected in the project, if applicable.[26] How is it achieved that everyone in the project team understands which legislation, ethical guidance and codes of practice referring to data handling apply in which ways to the project?						

[26] Of course, these general questions must be further detailed by going through the mentioned principles, responsibilities and rights. For doing so, numerous further guiding questions may also be retrieved, for example, from a valuable literature overview by Niall Sclater (2014), in particular questions that go into more detail and refer to the implementation status of data ethical principles and rights.

References

Corrin, L., Kennedy, G., French, S. Buckingham Shum, S., Kitto, K., Pardo, A., West, D., Mirriahi, N. and Colvin, C. (2019) *The Ethics of Learning Analytics in Australian Higher Education. A discussion paper*. Available at https://www.siyaphumelela.org.za/documents/5cc17266a030a.pdf (accessed 30 September 2020).

DDCMS (Department for Digital, Culture, Media and Sport) (2018) *Data Ethics Framework*. London: United Kingdom. Available at https://www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework (accessed 30 September 2020).

EC (EU Commission) (2016) *General Data Protection Regulation* (GDPR). As of 4 May 2016; entry into force 25 May 2018. Available at https://gdpr-info.eu/ and https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed 30 September 2020).

ICO (Information Commissioner's Office) (2019) *Guide to the General Data Protection Regulation* (GDPR). Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/ (accessed 30 September 2020).

Kleimann, B. (2019) (German) Universities as multiple hybrid organisations. *Higher Education* 77, 1085-1102. Available at https://doi.org/10.1007/s10734-018-0321-7 (accessed 30 September 2020).

Leiber, T. (2019) Organisational change and development through quality management in higher education institutions: Theory, practice, and recommendations for change agents. In: Hamlin, R.G., Ellinger, A.D. and Jones, J. (Eds.) *Evidence-Based Initiatives for Organizational Change and Development*. Hershey: IGI Global, pp. 316-341. See also: https://www.igi-global.com/book/evidence-based-initiatives-organizational-change/197443 (accessed 30 September 2020).

Leiber, T. and Meyer, W. (2019) Ethics in evaluation and ethical aspects of the standards for evaluation [in German]. In: Hense, J.U., Böttcher, W., Kalman, M. and Meyer, W. (Eds.) (2019) *Evaluation: Standards in different fields of action. Uniform quality standards despite heterogeneous practice?* [in German] Münster: Waxmann, pp. 87-104.

Leiber, T., Stensaker, B. and Harvey, L. (2018) Bridging theory and practice of impact evaluation of quality management in higher education institutions: a SWOT analysis. *European Journal of Higher Education* 8(3), 351-365.

NFES (National Forum on Education Statistics) (2010) *The Forum Guide to Data Ethics*. Available at https://nces.ed.gov/pubs2010/2010801.pdf (accessed 30 September 2020).

Sclater, N. (2014) *Code of Practice for Learning Analytics. A literature review of the ethical and legal issues*. London: JISC. Available at http://www.wojde.org/FileUpload/bs295854/File/07rp_54.pdf (accessed 30 September 2020).

Sclater, N. (2017) *Learning Analytics Explained*. London: Routledge.

SQELT (Sustainable Quality Enhancement in Higher Education Learning and Teaching) (2020) *Sustainable quality enhancement in higher education learning and teaching. Integrative core dataset and performance data analytics*. Erasmus+ Strategic Partnership. Available at https://www.evalag.de/sqelt (accessed 30 September 2020).

Tranberg, S., Hasselbalch, G., Kofod Olsen, B. and Byrne, S. (2018) *Data ethics. Principles and guidelines for companies, authorities and organisations*. AKAPRINT.