# Let’s Talk Ethics: Privacy and Data Protection Framework for a Learning Analytics Toolbox

Christina M. Steiner, Michael D. Kickmeier-Rust, Dietrich Albert
Knowledge Technologies Institute,
Graz University of Technology, Austria
{christina.steiner, michael.kickmeier-rust, dietrich.albert}@tugraz.at

## ABSTRACT

To find a balance between learning analytics research and individual privacy a learning analytics project needs to appropriately address privacy and data protection issues and comply with relevant legal regulations. A range of general guidelines, model codes, and principles for appropriate data and privacy protection exist that may serve the consideration of these topics in a learning analytics context. The importance and significance of data protection are also reflected in national and international laws and directives, where data protection is usually considered as a fundamental right. Existing ethics guidelines and approaches and relevant regulations served as a basis for elaborating a privacy and data protection framework for the LEA’s BOX project. A set of eight principles has been defined to derive implications to ensure an ethical treatment of personal data in the learning analytics platform and services.

## Keywords

Learning analytics, ethics, privacy, data protection.

## 1. INTRODUCTION

Learning analytics are key emerging technologies in education (Johnson et al., 2014) and their potential to optimize educational planning and processes, to inform and tailor teaching, and to inform and support learning has been highlighted by many authors (e.g. Ferguson, 2012; Greller & Drachsler, 2012; Long & Siemens, 2011). Educational institutions have always analysed the data of their students to some extent. Learners today have access to a multitude of learning tools, applications, and resources, they enhance their learning experience in virtual or simulated environments, and they connect to others through social media. All those interactions and resources may be captured and those multi-faceted learning processes can (potentially) be analysed using big-data analytics techniques (Pardo & Siemens, 2014).

With the advent and increasing capacity and adoption of learning analytics an increasing number of ethical and privacy issues also arise. For example, the evolution of sensors and new technologies enables a multi-faceted tracking of learners’ activities, location etc., such that more and more data can potentially be collected about individuals, who are oftentimes not even aware of it. Data collection and use under such circumstances is, of course, ethically and legally questionable (Greller & Drachsler, 2012). Ethical issues in learning analytics include the collection of data, informed consent, privacy, de-identification of data, transparency, data security, interpretation of data, as well as data classification and management (Slade & Prinsloo, 2013). These issues have been dealt with some tension so far (Pardo, 2014). There is a need to develop a clear and agreed set of ethical guidelines with respect to the ownership of data and analytic models, rights and responsibilities (Ferguson, 2012). At the moment there are no standard methods and procedures for informed consent, opting out etc. In fact, the need for a clearly defined and uniform approach and code of ethics to appropriately deal with the topics of ethics, privacy and learning analytics is increasingly being acknowledged (Berg, 2013).

LEA’s BOX is a research and development project funded by the European Commission and is dedicated to developing a learning analytics toolbox that will enable educators to perform competence-centred, multi-source learning analytics. In this paper we outline the privacy and data protection considerations and policy in the project. To find a balance between learning analytics research and individual privacy the project needs to appropriately address privacy and data protection principles and comply with relevant legal regulations. As a basis for establishing the requirements and implications for privacy and data protection different sources of information have been used.

This paper is structured as follows: Section 2 summarises privacy and ethical issues in learning analytics. Section 3 then outlines existing approaches or frameworks for dealing with these topics and in Section 4 an overview of privacy and data protection regulations is given. Section 5 presents the LEA’s BOX ethical framework, which is based on these resources and on input from an external ethics expert. The framework comprises a set of privacy, data protection, and ethical principles, which define requirements for the project’s learning analytics research and development. Finally, conclusions on the presented work are made (Section 6).

## 2. ETHICAL ISSUES IN LEARNING ANALYTICS

Relevant ethical issues and dilemmas in learning analytics can be summarised and grouped into the following overlapping areas (Campbell, DeBlois & Oblinger, 2007; Pardo & Siemens, 2014; Sclater, 2014; Slade & Prinsloo, 2013; Willis, 2014):

**Privacy**: The possibility that actions and personal data are tracked causes concerns in users. On the other hand, users may not be fully aware of the data being collected or exchanged when using technology services.

**Informed consent, transparency, and de-identification of data**: This relates to the question whether an individual needs to give consent to data collection and analysis, the obligation to inform about the data being collected and analysed, and the relevance and implication of de-identification of data.

**Location and interpretation of data**: Learning activities today are usually spread over different tools and locations and learning analytics aims at bringing together these different data sources for a more complete picture of learning. Questions arise on the implications of using multiple and non-institutional sources, and whether the data is representative of a particular student.

**Management, classification and storage of data**: This area relates to questions of data management, access rights, and the measures and level of data protection needed. It also involves the issue of the temporality of data.

**Data ownership**: This relates to the question who the owner of the data collected, of the analytics models, and the analytics output is. It also links to the aspect of outsourcing and data transfers to third parties and related regulations and responsibilities.

**Possibility of error**: Analytics results are always based on the data available and the outputs and predictions obtained may be imperfect or incorrect. Questions on the ramifications of making an error arise and what the implications of ineffective or misdirected interventions as a result of faulty analytics results are.

**Role of knowing and obligation to act**: Learning analytics brings new knowledge and insights about learning. The question arises, whether the gained knowledge entails responsibility to act on this information, and what the ramifications of action or inaction are.

# 3. EXISTING APPROACHES

## 3.1 Big Data and Ethics

Privacy and ethics have evolved important and pressing topics not only in learning analytics, though, but in analytics and big data in general (Schwartz, 2011; PMCA, 2013). "Big data poses big privacy risks," as Tene and Polonetsky (p. 251) put it. Data has become resource of important economic and social value and the exponentially growing amount of data (from a multitude of devices and sensors, digital networks, social media etc.) that is generated, shared, transmitted and accessed, together with new technologies and analytics available opens up new and unanticipated uses of information. The collection of large and multifaceted data sets and the new possibilities of their use lead to growing privacy concerns in data subjects and the disclosure and use of personal data is increasingly associated with fear, uncertainty, or doubt (Dirndorfer Anderson & Gardiner, 2014). Users are concerned about privacy and that large amounts of their personal information may be tracked and made accessible for other purposes to other users (Kobsa, 2007). On the other hand, social media are deeply integrated into users' daily lives and routines (Debatin, Lovejoy, Horn, & Hughes, 2009) and people, in fact, are willing to share a lot of personal details via these networks. Privacy attitudes and privacy behaviours, thus, often differ (Stutzman & Kramer-Duffield, 2009), which is called the "privacy paradox" (Barnes, 2006) and is evident when comparing users' self-reports about their understanding of caution regarding privacy settings and their actual, unconcerned behaviour of usually just keeping default settings without taking the opportunity of updating them to their needs and preferences (Debatin et al., 2009). So, privacy attitude and privacy behaviour are not necessarily conforming - people may not act according to the privacy preferences they claim. Usually they appear to be unconcerned about data protection and privacy until it is breached (Spiekerman & Cranor, 2009). Importantly, users' concerns about privacy also differ depending on the kind of data being collected, the context, and the perceived value of disclosing personal data (Pardo & Siemens, 2014).

In their article, Tene and Polonetsky (2013) elaborate on fundamental principles of privacy codes and legislation and argue that the principles of data minimisation and individual control and context need to be somewhat relaxed in a big data context and considered not only from an individual but also societal perspective (e.g. public health, environmental protection), while at the same time emphasizing transparency, access, and accuracy. The authors also discuss the distinction between identifiable and non-identifiable data and consider de-identification methods (anonymisation, pseudonymisation, encryption, key-coding) as an important measure for data protection and security.

The analytics process – regardless of the specific domain of application – aims at converting data into actionable knowledge and, in general, includes data collection (gathering information), integration and analysis (aggregating data from multiple sources and examining the data for patterns), decision making based on the information gained (act on the results of integration and analysis stage), and review and revision of analytics models. Schwartz (2011) has developed a set of ethical principles for analytics based on a series of interviews with experts in the field of data privacy, legislation, and analytics. These include a set of overarching ethical standards:

- Compliance with legal requirements,
- Compliance with cultural and social norms,
- Accountable measures tailored to identified risks
- Appropriate safeguards to protect the security of data
- Responsible limits on analytics in sensitive areas or with vulnerable groups

Besides specifying these generic principles, Schwartz in particular argues that at different stages of the analytics process different ethical considerations are relevant. Accordingly, the rules how to tackle these challenges need to be tailored to each analytics stage – always aiming at maximising good results and minimising bad ones for the persons whose data is processed. In data collection, care needs to be taken about the kind of information; in particular avoiding the collection of sensitive data. For data integration and analysis a sufficient data quality should be ensured and anonymisation should be done, as appropriate. In decision making it needs to be made sure that the analytics results on which decisions are based are reasonably accurate.

## 3.2 Ethical Frameworks in Learning Analytics

Researchers have started to discuss ethical and privacy issues and principles specifically for learning analytics as a basis for advancing learning analytics in this direction. Still, although many authors mention ethical issues, there are only few coherent approaches elaborating ethical challenges in more detail and attempting to define an ethical framework to guide institutions, researchers and developers in the application of learning analytics (Slade & Prinsloo, 2013).

The topics of privacy and ethics are directly related to aspects of trust and accountability (Pardo & Siemens, 2014). A rational and sensible dealing with privacy and ethics is therefore needed to leverage learning analytics technologies in terms of broad practical adoption, acceptance, and growth. Reflection and deliberation with ethical questions need to be aligned with technical innovation in analytics, because the slow pace of law may not able to match the speed of innovation. Nevertheless, existing approaches on ethics in learning analytics commonly and understandably ground their discussion within and relating to legalities and legal understanding of privacy (Willis, 2014).

One possible approach of elaborating the ethical issues of learning analytics is to determine and analyse the risks of implementing a learning analytics project and how to manage them. Stiles (2012) identifies a set of specific areas and associated risks. Data protection is considered as a key risk to be addressed, including the aspects of privacy, security, governance, and compliance. To ensure privacy, security, quality, auditability of data an appropriate level of control needs to be implemented (i.e. data and information governance – for example through policy, checklist). Compliance with legal requirements on data privacy and security creates increased data awareness, quality, and protection (i.e. data and information compliance). The risks associated with these areas need to be appropriately addressed for the implementation and use of analytics in an educational organisation.

Greller and Drachsler (2012) have considered ethical and legal aspects in their framework for learning analytics under the dimension of 'external constraints'. Apart from ethical, legal, and social constraints, they also consider organisational, managerial, and process constraints as relevant components on this dimension. These external limitations can be categorised into conventions (ethics, personal privacy, and other socially motivated constraints) and norms (restrictions by law or mandated standards and policies). This makes clear that there is a reasonable distinction but close linkage between ethics and legal regulations: Ethics deals with those measures that are morally allowed; the law defines what is allowed without legal consequences (Berg, 2013). In many cases ethical issues are reflected in legislation, but ethical considerations go beyond what is set in laws and depend on ideological assumptions and epistemologies (Slade & Prinsloo, 2013). Many legal regulations are based on ethics, and in particular situations an ethical position needs to be applied for interpreting the law (Sclater, 2014). Kay, Korn, and Oppenheim (2012) highlight that given the mission and responsibilities of education, "broad ethical considerations are crucial regardless of the compulsion in law" (p. 20).

Kay et al. (2012) outline that learning analytics is in the area of conflict between assuring educational benefits, business interests of and competitive pressure on educational institutions, and expectations of the born digital generations of learners. They postulated four key principles for good practice with respect to ethical aspects and analytics when dealing with these conflicts:

- **Clarity**: definition of purpose, scope and boundaries
- **Comfort and care**: consideration of interests and feelings of the data subject
- **Choice and consent**: information and opportunity to opt-out or opt-in
- **Consequence and complaint**: acknowledging the possibility of unforeseen consequences and mechanisms for complaint

Willis, Campbell and Pistilli (2013) refer to the area of conflict and a need for balancing between faculty expectations, privacy legislation, and an educational institution's philosophy of student development, when dealing with ethical questions. They do not define specific guidelines on different ethical issues, but suggest using the Potter Box, a flexible ethical framework commonly applied in business communications, to deal with the ethical dilemma of analytics. This approach, in fact, only provides a thinking framework for analysing a situation but does not provide one clear solution to ethical dilemmas. The Potter Box foresees four universal steps when taking ethical decisions on specific questions, as described in Table 1.

Slade and Prinsloo (2013) take a socio-critical perspective on the use of learning analytics in their article elaborating on ethical issues. They propose a framework of six principles to address ethics and privacy challenges in learning analytics:

- **Learning analytics as a moral practice**: Focus should not only be put on what is effective, but on supporting decisions about what is appropriate and morally necessary. The ultimate goal is understanding, not measuring.
- **Students as agents**: Students should be involved in the learning analytics process as collaborators and co-interpreters. A student-centric approach to learning analytics is recommended.
- **Student identity and performance are temporal dynamic constructs**: The dynamicity of data is acknowledged, thus providing only a snapshot view of a learner at a particular point in time in a particular context.
- **Student success is a complex and multidimensional phenomenon**: Learning progress and success consists of multidimensional, interdependent interactions and activities. The data used in learning analytics is incomplete and analytics may lead to misinterpretation or bias.
- **Transparency**: Information about the purpose of data usage, data controllers/processors, and measures to protect the data should be provided.
- **(Higher) education cannot afford not to use data**: Information that learning analytics may provide should not be ignored by an educational institution.

Pardo and Siemens (2014) have analysed ethical and privacy issues in learning analytics research in educational institutions and have also taken into account how privacy and ethics are addressed in other contexts. They identify a set of four principles that aggregate numerous issues and are intended to serve as a basis for setting up appropriate mechanisms for meeting ethical and legal requirements when developing and deploying learning analytics. When applying these principles, this needs to be done in due consideration of legal and social requirements. The four principles are:

- **Transparency**: All stakeholder groups in learning analytics, i.e. learners, teachers, educational administrators, should be provided with information on what type of data is collected and how it is processed and stored.
- **Right to access**: Security of data needs to be guaranteed. Access rights need to be clearly defined for a data set.
- **Student control over data**: This refers to giving users the right of users to access the data collected about them and, if necessary, to correct it.

**Accountability and assessment**: The analytics process should be reviewed and for each aspect of the learning analytics scenario the responsible entities should be identified.

Table 1: The Potter Box.

| | |
|---|---|
| **Definition**:<br>The empirical facts of a given situation are clearly defined without making any judgements. | **Loyalties**:<br>Loyalties are chosen, for example people affected by a situation (application of learning analytics), entities acting on the gained information, responsible persons in case of failure etc. |
| **Values**:<br>Values representing conventions, rights, and beliefs are identified and compared (e.g. moral values, professional values). Differences in perspectives of stakeholders involved can be analysed. | **Principles**:<br>A set of ethical principles (e.g. Mill's principle of utility – 'Seek the greatest happiness for the greatest number') is identified and considered that are applicable to the situation in question. |

## 3.3 General Ethical and Privacy Guidelines Models

The OECD guidelines have been indicated as relevant source of basic principles when seeking guidance on how to deal with privacy issues in analytics technologies and other systems (Spiekermann & Cranor, 2009; Tene & Polonetsky, 2013). In 1980, the OECD (Organisation of Economic Co-Operation and Development) provided the first internationally agreed collection of privacy principles, aiming at harmonizing legislation on privacy and facilitating the international flow of data. The set of eight basic guidelines mirrored the principles earlier defined by the European Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data and addressed (Levin & Nicholson, 2005). The basic OECD principles are (OECD, 2013b, p. 14-15):

- **Collection limitation**: There should be limits to the collection of personal data. Data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data quality**: Personal data should be relevant to the purposes for which they are to be used, and to the extent necessary for those purposes. Data should be accurate, complete and kept up-to-date.
- **Purpose specification**: The purposes for which personal data are collected should be specified not later than at the time of data collection. Subsequent use should be limited to the fulfilment of those purposes or compatible purposes.
- **Use limitation**: Personal data should not be disclosed, made available or used for purposes other than specified – except with the consent of the data subject or by the authority of the law.
- **Security safeguards**: Personal data should be protected by reasonable security safeguards against loss or unauthorised access, destruction, use, modification, or disclosure.
- **Openness:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Information on the existence and nature of personal data, purpose of their use, and the identity and location of the data controller should be available.
- **Individual participation**: Individuals should have the right to obtain confirmation of whether or not data relating to them is held and to have communicated to them the data, to be given reasons if a request is denied, and to challenge data relating to them and to have the data erased, rectified, completed or amended.
- **Accountability:** The data controller should be accountable for complying with measures, which give effect to the above principles.

The OECD guidelines were not binding for OECD members, but have gained legal significance and served as a basis for privacy legislation in Europe (European Parliament, 1995; Levin & Nicholson, 2005; Spiekermann & Cranor, 2009). The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 2013b), an update of the original version from 1980, which constituted the revision, keeps the original "Basic Principles" of the guidelines, while modernising considerations on transborder data flows and strengthening privacy enforcement. The updated guidelines focus on the practical implementation of privacy protection through an approach grounded in risk management. Furthermore, the need for greater efforts to address the global dimension of privacy through improved interoperability is acknowledged.

Currently, the OECD is working on privacy-related issues in the context of large-scale data use and analytics. In a preliminary report (OECD, 2013a) on the broader topic of 'data-driven innovation as a new source of growth' different sectors of data use and analytics are elaborated (online advertisement, health care, utilities, logistics and transport, and public administration), however without any specific reference to learning or academic analytics. Privacy protection is indicated as one of several areas that need public policies and practices to leverage the potential of big data. Privacy protection enabling open, secure, reliable, efficient, and also cross-border flows of data on the one hand, and reducing privacy risks and enhancing responsible behaviour in the use of personal data is called for on the other hand.

Based on the framework of the OECD Guidelines, the Federal Trade Commission of the United States has defined the Fair Information Practice Principles (FIPP), which specify concepts of fair information practice in electronic marketplace. These cover five core principles of privacy protection, which many other guidelines and reports on fair information practice have in common, and are therefore relevant for information practice in dealing with personal information, in general (Federal Trade Commission, 1998):

- **Notice/Awareness**: Users need to be informed before personal data is collected from them. Giving notice is necessary in order to enable the data subject to consciously decide whether he/she wants to disclose personal information, and to what extent. This principle is considered the most fundamental one, since the other principles are only meaningful provided that the user has notice.
- **Choice/Consent**: This principle refers to giving data subjects options as to how personal data collected from them may be used, e.g. secondary use. Thereby, traditionally two approaches may be taken, opt-in or opt-out.
- **Access/Participation**: This principle relates to giving users the possibility to access their data and to ensure that the data is accurate and complete.
- **Integrity/Security**: Data needs to be accurate and secure and appropriate steps and safeguards need to be taken to ensure that, e.g. using reliable data sources, cross-referencing multiple sources.
- **Enforcement/Redress**: To ensure compliance to privacy protection principles, there need to be enforcement and redress mechanisms through self-regulatory regimes, legislation creating private remedies for users, or government enforcement.

Ethical issues in learning analytics may also be considered in the context of the history of internet research ethics, where the attempt of finding a balance between harms to the individual and greater scientific knowledge has been made (Slade & Prinsloo, 2013). The Association of Internet Researchers provides a set of ethical guidelines for decision making about internet research (Ess & AoIR, 2002; Markham & Buchanan, 2012). These are aimed at providing researchers a basis for conducting their research in an ethical and professional manner and have also been indicated by learning analytics researchers as a valuable source for dealing with privacy issues in the application of learning analytics.

## 3.4 Ethics by Design

Since learning analytics involves technology, ethics and privacy concerns may not purely be considered from a legal perspective, but need to be addressed from a technological point of view (Pardo & Siemens, 2014). One way of ensuring that is to take privacy and ethics, in general, into account already during the design process of learning analytics tools[1]. This approach is called ‘privacy by design’, ‘value-sensitive design’ or ‘ethics by design’ and it has been started to be acknowledged and taken up also in learning analytics research (e.g. Bomas, 2014; Scheffel, Drachsler, Stoyanov, & Specht, 2014).

Value-sensitive design or ethics by design corresponds to the approach of incorporating ethical and legal requirements and considerations in the design and development process, i.e. making them an inherent part of the software being created (Friedman, 1997). This approach deals with design principles and guidelines so that the software itself follows ethical rules or support humans to follow ethical rules (Gotterbarn, Miller, & Rogerson, 1997; Gotterbarn, 1999). Privacy by design, more concretely focuses on privacy engineering and developing guidelines for designing and developing privacy-friendly systems (Cavoukian, 2011). Spiekermann and Cranor (2009) have carried out a privacy requirements analysis that is applicable to a wide variety of systems and identify system activities typically performed by information systems and their impact on user privacy. This impact depends on how the system activities are performed, what type of data is used and who uses it, and which privacy spheres are affected. Guidelines are provided on how notice, choice, and access can be implemented as fair information practices and users can be informed about them. Relating to these guidelines, in ethics by design a ‘privacy-by-policy’ approach (focus on implementation of notice and choice principles) and a ‘privacy-by-architecture’ approach (focus on minimizing collection of identifiable personal data and anonymisation) can be distinguished (Spiekermann & Cranor, 2009).

# 4. PRIVACY AND DATA PROTECTION REGULATIONS

Legislation on privacy and data protection is regulated in national and international information privacy and data protection laws, which address the protection prohibiting the disclosure or misuse of information held on private individuals. Regulations started to appear in countries with high spread and use of the internet (Pardo & Siemens, 2014). Examples are the European Union Directive on the protection of individuals with regard to processing of personal data and the free movement of such data (European Parliament, 1995), the Canadian Personal Information Protection and Electronic Documents Act (Government of Canada, 2004), the Australian Privacy Act and Regulation (Australian Government, 1988, 2013), or the US Consumer Data Privacy in a Networked World (The White House, 2012). The Family Educational Rights and Privacy Act (US Government, 2004), an US federal law, is a legislation that specifically applies to education, i.e. the protection of the privacy of student education records. This law allows the use of data on a need-to-know basis and provides parents certain rights of access to their children's education records.

In parallel with legislative efforts to data protection, non-profit organisations evolved that aim at defending user digital rights (Pardo & Siemens, 2014); for example the ARGE DATEN Privacy Service[2] in Austria or the Electronic Frontier Foundation[3] and Privacy Rights Clearinghouse[4] in the US.

There is a general awareness of the importance and significance of data protection, and this is reflected in many national and international documents, where data protection is considered a fundamental right (Rodotà, 2009). Nevertheless, “the right to data protection is not an absolute right; it must be balanced against other rights” (FRA, 2014, p. 21), i.e. it needs to be considered and implemented always in relation to its function in society.

Providing a comprehensive description of the legislation initiatives on privacy and data protection of personal data is beyond the scope of this paper (an overview and comparison between international privacy laws and approaches is given, for example, in Levin and Nicholson (2005) and Movius and Krup (2009)). Instead, only reference to the relevant European legislation shall be given, which aims at providing a unified initiative for EU members.

## 4.1 European Regulations

The transfer of personal data between countries in the EU is necessary in day-to-day business of companies and public authorities. Since conflicting data protection regulations of different countries might complicate international data exchanges, the EU has established common rules for data protection[5]. The application of this European legislation is monitored by national supervisory authorities.

The European data protection legislation considers the protection of personal data as a fundamental right. Current EU law is the 1995 Data Protection Directive ((European Parliament, 1995), which applies to countries of the European Economic Area (EEA; i.e. all EU countries plus Iceland, Liechtenstein and Norway). The directive seeks to keep a balance between a high level of protection of individual privacy and the movement of personal data within the European Union. It applies to data that is collected and processed automatically (e.g. computer database) and in non-automated ways (traditional paper files). This directive refers to the national law applicable and indicates that each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data.

The EU Data Protection Directive defines rules for international transfers of personal data to countries outside the EU/EEA. Data transfer outside the EU/EEA may only be done under the precondition that an adequate level of protection is guaranteed. Standard contractual clauses have been defined for transfers to data controllers and processors outside the EU/EEA. The Directive has been extended by a specific directive for data communication in the electronic communication sector[6] (ePrivacy directive) to address the specific requirements with respect to privacy and data protection in the context of information and communication technologies, especially the internet and electronic messaging services. This directive shall help to ensure that users can trust the services and technologies they use for electronic communication. The main regulations covered by the Directive apply to spam, ensuring the user’s consent, and the installation of cookies.

The European Commission is currently in process of establishing a reform of the data protection legislation, to enforce protection of personal data by updating and modernising data protection rules.

[1] e.g. https://www.privacybydesign.ca/

[2] http://www.argedaten.at

[3] https://www.eff.org/

[4] https://www.privacyrights.org/

[5] http://ec.europa.eu/justice/data-protection/index_en.htm

[6] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058

# 5. THE LEA’S BOX PRIVACY AND DATA PROTECTION FRAMEWORK

The LEA’s BOX project (www.leas-box.eu) focuses on researching and developing novel approaches to competence-centred learning analytics and visualizations. Based on psycho-pedagogical knowledge representation frameworks and the review of existing learning analytics and educational data mining approaches, as well as open learner modelling techniques, conceptual research on analytics and visualization methods is carried out and translated into the technical development and integration of a toolbox of services for empowering teachers and learners. In this section we present the privacy and data protection framework of LEA’s BOX. The established framework shall assure that the learning analytics toolbox and platform developed work in accordance with national privacy policies and regulations on data protection and state of the art and best practice approaches of dealing with ethical and legal aspects.

Thus, three main sources of information have been used to inform the establishment of this framework:

- state of the art approaches and guidelines to deal with ethical and privacy issues (cf. section 3)
- relevant jurisdictions (cf. section 4); in LEA’s BOX, in addition to the European Directive, in particular the privacy and data protection regulations in Austria, Czech Republic, Turkey, and the United Kingdom have been considered
- project-specific discussion with an external ethics expert (cf. section 5.1 below)

The aim in defining the privacy and data protection framework was to translate these different types of resources into a coherent set of requirements for the LEA’s BOX project. These requirements should go beyond outlining philosophical ideals, but should actually be applied as ethical principles and feed into the design and development of the project’s technologies project (see Figure 1). In line with Schwartz (2011), the requirements shall represent an accountable approach reflecting the specific ethical and data protection issues relevant for the project. They shall provide an appropriate frame for researching and exploring the educational possibilities to benefit from learning analytics without sacrificing privacy (Bomas, 2014).

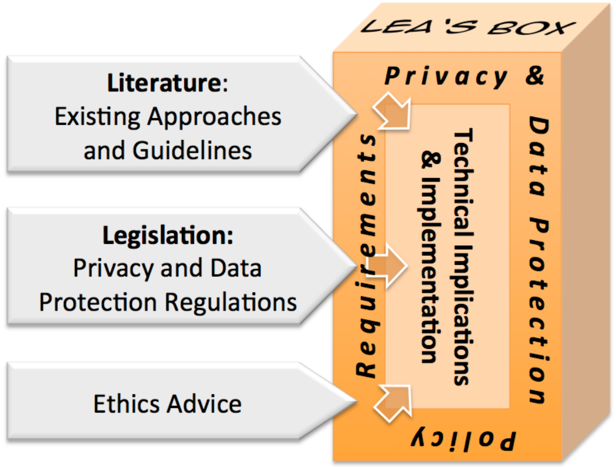
Literature:
Existing Approaches and Guidelines
Legislation:
Privacy and Data Protection Regulations
Ethics Advice
LEA'S BOX
Privacy & Data Protection Policy
Requirements
Technical Implications & Implementation

Figure 1: Privacy and data protection policy in LEA’s BOX.

## 5.1 Ethics Advice

An ethics expert is involved in LEA’s BOX as an external ethics advisor. This expert is the second chairman of the Ethics Commission of the University of Graz, Austria, and representative for natural sciences in this commission; he has been consulted on privacy and ethical aspects and questions related to the project’s research and development. Aside from discussing general ethical use of data, the importance and approaches to gathering data subjects’ consent and providing transparency, one topic evolved to be particularly relevant – the consideration of learning analytics as moral practice’ (H. Römer, personal communication, 27 November 2014). When researching new learning analytics approaches, in a first step the new methods and algorithms need to be tested and evaluated and should not directly affect data subjects; this means, an ethical use of learning data would imply that the results of the analysis must not have any direct impact on the learners. Only in a second step, after the methods could be validated, the implementation of consequences or interventions on the basis of the analytics results should be approached. This ethical perspective of validating learning analytics before using the results for decision making, in fact, stand in conflict with the moral value of an ‘obligation to act’ commonly discussed in the literature (e.g. Campbell et al., 2007; Kay et al., 2012; Willis et al., 2013) – i.e. the idea of an ethical duty to act on the information gained from learning analytics, like information about students at risk of dropping out. This position of validating a new learning analytics approach is directly related with the consideration that learning analytics may yield results that are not perfect or valid, but may be inaccurate or even incorrect (e.g. van Harmelen & Workman, 2012), and is in line with Schwartz (2011), who claims for big data, in general, that decision making in the analytic process needs to be grounded on reasonably accurate analytic output.

## 5.2 Privacy and Data Protection Principles

A set of principles relating to privacy, data protection, and ethics has been identified, which form an ethical and information practice framework for LEA’s BOX. These principles have been derived from a harmonization of existing ethical guidelines and approaches, complemented by the discussion points of the ethics advice, and in alignment with the aspects of data protection and privacy covered by national and European regulations. Ethical and privacy principles from these different resources have been mapped to each other. The eight principles derived for LEA’s BOX were formulated based on this integration of privacy and data protection resources and the identification of the key aspects.

### *5.2.1 Data Privacy*

The first and overarching requirement for LEA’s BOX is data privacy, in line with the fundamental right to data protection as reflected in national regulations and the EU data protection directive (Rodotà, 2009). Collection and use of personal data need to be fair and provide appropriate protection of privacy. Information on privacy and data protection practices should be available and easily understandable.

Users having the feeling their privacy is endangered may show resistance (Greller & Drachsler, 2012). To give them the feeling that their data is used in an acceptable and compliant way, policies and guidelines to protect the data from abuse are needed and need to be communicated. The protection of data with respect to data collection and analysis is ensured by legislation and by additional institutional privacy regulations (Campbell et al., 2007), as represented by the privacy principles at hand.

### 5.2.2 Purpose and Data Ownership

An adequate specification and documentation of the purpose of data processing needs to be ensured in LEA's BOX at any stage, and must be made available. The purpose and boundaries of a learning analytics application should be clearly defined and available before processing is started. "Processing personal data for undefined and/or unlimited purposes is unlawful" (FRA, 2014, p. 68). In essence, considering learning analytics as a moral practice, learning analytics should aim at supporting learners (e.g. Slade & Prinsloo, 2013; The Open University, 2014). When researching new learning analytics methods, though, establishing and ensuring reasonable accuracy of analytics results (i.e. creating truly actionable knowledge) represents the ethical standard to be addressed first (H. Römer, personal communication, 27 November 2014; Schwartz, 2011), before dealing with ethical questions on the responsibility to act or not act based on the new knowledge gained (e.g. Willis, 2014).

Another relevant ethical aspect is data ownership. It has been argued that in this regard there is a lack of legal clarity, when considering learning analytics applications (Greller & Drachlser, 2012). Traditionally, the data collected about a person, i.e. before anonymisation, belongs to the owner of the data collection tool (data client). Meanwhile, there is a trend of considering users as the owners of the data collected about them and institutions are borrowing them for a clearly stated purpose. In learning analytics things get more complicated very quickly, since usually data from a whole population of learners is used to produce a prediction model – and the question arises, who the owner of such kind of model is (Pardo, 2014). So, even if the raw personal data is owned by the user, what about the information derived from it? While for raw learning data there is no issue of copyright, copyright and database rights may be relevant for enhanced learning data (e.g. collations of data, prediction models). The owner of any IPR is typically the institution that has collected (and enhanced) the data (Kay et al., 2012).

The question of data ownership is also further complicated when thinking of the integration of learning data from different sources, which may potentially mean different organisations/data clients. It has been argued that to fully exploit the potential of learning analytics and build a holistic picture of an individual's learning (e.g. Ferguson, 2012; Dyckhoff, 2011), data integration is needed – e.g. institutionally held student data with learning data from educational tools.

It has been argued that, in fact, the concept and consideration of data ownership may not be most appropriate and helpful, but more relevant are the notions of data controller and data processor as used in data protection regulations (Sclater, 2014). Data controller is a natural or legal person, or an authority, that processes personal data and determines the purpose of processing. The data subject has the right to be provided with information about the identity of the data controller (including contact details) and purposes of processing. A data processor is a separate legal entity, who processes personal data on behalf of the controller (FRA, 2014).

### 5.2.3 Consent

LEA's BOX needs to apply appropriate techniques for gathering consent from students and parents, as a legal basis for processing personal data. Informing users about the collection of their data and gathering their consent need to be realised as a basic ethical principle and procedure (Greller & Drachsler, 2012). It has been argued that in learning analytics there should be virtually no reasons to waive informing users about the use of their data and to set up a clear policy of informed consent (Slade & Prinsloo, 2014). According to current privacy legislation the collection of consent also needs to be implemented for the use of Cookies.

Consent needs to be free, informed, specific and given unambiguously. Sufficient information needs to be provided to the data subject, to assure he/she is clearly informed about the object and consequences of consenting before taking the decision. Information needs to be precise and easy to understand. Consent given non-explicitly on the basis of inactivity (passive consent from parents) is usually not considered as unambiguous and should be avoided (FRA, 2014; H. Römer, personal communication, 27 November 2014). Although the European regulations do not explicitly mention a general right to withdraw consent at any time, it is widely presumed and accepted that such right exists (FRA, 2014).

The principle of consent refers to giving data subjects the possibility to agree/disagree to a data collection and application. The information provided as a basis for gathering consent should establish a balance between allowing research and protecting users from potential harm and thus, may refer to "a broad definition of the range of potential uses to which a student's data may be put" (Slade & Prinsloo, 2014).

### 5.2.4 Transparency and Trust

Transparency is probably the issue that relates to most concerns in ethical considerations on learning analytics (Pardo & Siemens, 2014). While privacy legislation requires learners' consent for data collection, the principle of transparency goes beyond that. Data subjects (i.e. usually learners, but also teachers) should be given notice about what kind of data is gathered and recorded, and should be provided with information on how the analytic processing is done. Transparency also means to provide information on data management procedures, on how data is dealt with after its primary purpose, and whether information is transmitted to outside an institution. Users should, however, not only be informed about how their data is used outside an educational institution, but also within the institution (Slade & Prinsloo, 2013). In addition, data subjects should also be made aware of the possible outcomes of the data application and the measures of data protection taken (Willis & Pistilli, 2014).

The following information is considered essential to consider data subjects as properly informed (Federal Trade Commission, 1998): the entity collecting the data, the uses to which the data will be put, potential recipients of data, the type of data collected and data collection method, consequences of refusal, and measures taken to ensure data quality and security. Frequently also information on consumer rights is included. In case of learning analytics, an appropriate and understandable description of the analytic models/procedures should be provided (H. Römer, personal communication, 27 November 2014). Data subjects should be enabled to understand what is happening with their data (FRA, 2014).

Informing users about what kind of data is recorded and for what purpose is not only an important ethical and legal privacy principle in LEA's BOX, but it is also key to foster trust in data subjects – for learning analytics, and for the educational institution applying it. If users trust the learning analytics technology, because they understand the data application and the (potential) value and usefulness it may have to them, users' experience and acceptance is considerably enhanced (Pardo & Siemens, 2014). As a result, the application of the principle of transparency should also include information on the potential benefits (or harms) due to the data application, to raise users' awareness and understanding of the learning analytics approach and, potentially, involve them as active agents in the implementation of learning analytics.

### *5.2.5 Access and Control*

In addition to gathering users' consent and providing transparency of when and how data is collected and analysed, data subjects should be given control of their own data. This forms the fifth principle of our framework. Access and control mean users should be given access to the data collected about them, and the opportunity to correct them, if necessary. The principle of access and participation is reflected in legislation as a right of the data subject. While giving access is completely in line with the idea of transparency, the aspect of modifying data is somewhat challenging in learning analytics and only applies to certain types of data – i.e. data from plain observations, but not necessarily summaries or results obtained from data. Procedures for correction or deletion of personal data, if inaccurate, misleading, or out-dated, need to be provided to users.

In fact, some authors have even claimed to establish a culture of participation, to consider learners as agents sharing responsibility for the accuracy, maintenance, and up-to-dateness of their student data; they may even be actively involved in the implementation of learning analytics and help shaping interventions (Slade & Prinsloo, 2013; The Open University, 2014). This requires a clear plan and procedure of communication with learners.

Dashboards and open learner models are approaches of visualising learning analytics data and results. They are often an inherent part of learning analytics approaches as instruments for reporting and fostering reflection (Bull & Kay, 2010; Verbert, Duval, Klerkx, Govaerts, & Santos, 2013). These visual approaches provide users with access to the data whenever and for how long they want and thus, offer transparency to data subjects on the data collected about the learning process (Pardo & Siemens, 2014). More recent approaches of negotiated user models reflect the idea of student control, since the open learner model is used to interactively negotiate and potentially update the content of the learner model. In LEA's BOX research on open learner model communication and negotiation is done, which can be considered a realisation and application of the ethical principle of access and participation.

Access and control over data need to be governed by technically implementing appropriate authentication mechanisms and the establishment of an access right structure. Simple and understandable procedures for indicating inaccurate data, for updates or corrections, and for verifying information need to be established and implemented in the management and maintenance of data files.

### *5.2.6 Accountability and Assessment*

Principles of data protection can only work with appropriate mechanisms to enforce and redress them (FRA, 2014). The institution, department or person responsible or accountable for a learning analytics application and its proper functioning need to be identified. In LEA's BOX a clear structure of responsibilities of individual partners and persons has been established from the outset of the project.

In addition, the learning analytics process should be evaluated in order to refine data collection, management, and analysis (Pardo & Siemens, 2014). The overarching goal of learning analytics is to better understand learning processes and to optimise and support learning and teaching. This can only be achieved when ensuring correctness of the data and analytics algorithms. A constant reviewing and adjusting of analytics methods will increase the accuracy of results and suitability of the learning analytics process and maximise impact (Pardo, 2014; van Harmelen & Workman, 2012). The importance of the review and revision stage in analytics is also highlighted by Schwartz (2011). Beside that, he also refers to the assessment of the impact of using analytics on the basis of stakeholders trust. In LEA's BOX a continuous assessment, refinement and enrichment of learning analytics methods and tools is targeted as a basis for on-going improvement. In addition to this validation and elaboration of data processing, impact on learners and teachers (e.g. in terms of acceptance) will be addressed in a series of pilot and evaluation studies.

### *5.2.7 Data Quality*

According to different ethics frameworks an appropriate quality of data needs to be ensured (e.g. Federal Trade Commission, 1998; OECD, 2013b; Pardo & Siemens, 2014). Data needs to be representative, relevant, accurate and up-to date. Information that is not up-to date cannot be assumed to be reliable or reflecting the current status of a learner and may thus lead to wrong conclusions from analytics (The Open University, 2014). An approach of sharing responsibility for the accuracy and maintenance of personal data between educational institution and learner (compare 'Access and Control') is considered reasonable for ensuring an adequate level of data quality.

Especially when gathering and combining data from multiple sources, care needs to be taken to use reliable sources. It needs to be acknowledged that the data collected may provide an incomplete picture of the learning process and only represents a snapshot in time and context. Bias and stereotyping need to be prevented by constantly taking into account the incomplete and dynamic nature of individual learning and experience (Slade & Prinsloo, 2014).

Beside an adequate quality of learning raw data, in LEA's BOX it needs to be ensured that data is used wisely for carrying out integration and analysis. Any interpretation, enhancement, or manipulation of data with the aim of extracting meaning will be grounded on a sound technique; the analytics models will be transparent and available for review and testing.

### *5.2.8 Data Management and Security*

In general, personal data needs to be treated and managed in a sensitive and ethical way in LEA's BOX. Data must be kept protected and secure at different levels and by adequate measures, in accordance with applicable jurisdictions. Accountability, thus, requires safeguards for data protection; compliance of data processing with data protection regulations needs to be demonstrated (FRA, 2014).

Appropriate measures need to be taken to protect the data against unauthorised access, loss, destruction, or misuse. This includes a clearly defined policy of who is authorised to access the data, to which parts of the data and the application, and which kinds of data operations are allowed (Pardo & Siemens, 2014). Processes for redress need to be provided to users in case of any unauthorised access or use of personal data. Preservation and storage of data needs to be aligned with national and EU regulations.

In line with this principle of data management and security, the effective governance and stewardship of data should be ensured and a clear and transparent structure of data shall be established in LEA's BOX. Security thereby needs to involve measures on a managerial and on a technical level (Federal Trade Commission, 1998; FRA, 2014). On the managerial level, internal organisational rules should be established that cover, for example regular information of employees about data security rules, obligations of confidentiality, a clearly defined structure of responsibilities and competencies in data processing and transfer, training on effective security precautions etc. Technical measures for data security relate to having the right equipment (hardware and software) in place, encryption in data transmission and storage, the use passwords to limit access, data storage on secure servers etc.

## 6. CONCLUSION

To conclude this paper, we want to reference Stephanie Moore (2008) who highlighted that ethics is a critical aspect, however, hard to tackle because it is full of variability, contradicting viewpoints, and squishy definitions. Specifically in the context of designing, developing, and deploying education software and in the context of making school studies, individual beliefs, values and preferences influence the scientific work.

The presented data protection and privacy framework provides the foundations for a proper code of conduct; in particular it needs to be assure that technology and tools developed in the project and also 3rd party technologies used are in line with these foundations. The principles defined form requirements for LEA's BOX and are translated into concrete technical implications and actual implementation. Thus, we transfer the respective principles into an approach of "ethics by design".

Despite the ethical challenges of learning analytics in general, and in the context of a research project that is developing novel tools and algorithms, in particular – *education cannot afford not to use (big) data*, to say it in the words of Sharon Slade and Paul Prinsloo (2013).

In the context of this complex and sensitive field, this paper cannot claim to be complete; for example, critical further aspects concern tracking of IP addresses, the accessing of individual data such as done by many Smartphone apps (e.g., GPS location), the identifiability of users among each other, or the access to webcams or chat functions (a critical introduction in the context of online gaming is given for example in the *iX Developer* journal, volume 1/2015). Still, the established framework provides the project's 'personal' code of conduct, strengthens our 'personal' awareness, and derives a number of concrete technical requirements. The framework is considered also relevant to learning analytics at a larger scope and may be adopted as a starting point and theoretical basis also for other learning analytics initiatives. While the way how these principles are actually applied and implemented may take different forms, compliance with the current laws and regulations shall be ensured at any stage of the project as a main requirement of privacy and data protection. The principles defined in our framework need to be aligned with the very specific context of a concrete learning analytics application in question. Tene and Polonetsky (2013) talk about "levers that must be adjusted to adapt to varying … conditions" (p. 242).

## 7. ACKNOWLEDGMENTS

The work presented in this paper is supported by the European Commission (EC) under the Information Society Technology priority of the 7th Framework Programme for R&D under contract no 619762 LEAs BOX. This document does not represent the opinion of the EC and the EC is not responsible for any use that might be made of its content.

## 8. REFERENCES

[1] Australian Government (1988). *Privacy Act 1988. No. 119, 1988 as amended*. Canberra: Office of Parliamentary Counsel.

[2] Australian Government (2013). *Privacy Regulation 2013*.

[3] Barnes, S.B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*. Retrieved December 10, 2014 from http://firstmonday.org/article/view/1394/1312

[4] Berg, A. (2013, August 21). *Towards a uniform code of ethics and practices for learning analytics* [Web log post]. Retrieved from https://www.surfspace.nl/artikel/1311-towards-a-uniform-code-of-ethics-and-practices-for-learning-analytics/

[5] Bomas, E. (2014, August 29). *How to give students control of their data.* [Web log post]. Retrieved from http://www.laceproject.eu/blog/give-students-control-data/

[6] Bull, S. & Kay, J. (2010). Open Learner Models. In R. Nkambou, J. Bordeau and R. Miziguchi (Eds.), *Advances in Intelligent Tutoring Systems* (pp. 318-338). Berlin: Springer.

[7] Campbell, J. P., DeBlois, P. B. & Oblinger, D. G. (2007). Academic analytics. *Educause Review, 42*, 1–24.

[8] Cavoukian, A. (2011). *Privacy by design. The 7 foundational principles. Implementation and mapping of fair information practices*. Information and Privacy Commissioner of Ontario. Retrieved December 12, 2014 from http://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf

[9] Debatin, B., Lovejoy, J.P., Horn, A.-K., & Hughes, B.N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-mediated communications, 15*, 83-108.

[10] Dirndorfer Anderson, T. & Gardiner, G. (2014). What price privacy in a data-intensive world? In: *iConference 2014 Proceedings* (pp. 1227-1230).

[11] Dyckhoff, A.L. (2011). Implications for learning analytics tools: A meta-analysis of applied research questions. *International Journal of Computer Information Systems and Industrial Management Applications, 3*, 594-601.

[12] Ess, C. & AoIR (2002). *Ethical decision-making and Internet research: Recommendation from the AoIR Ethics Working Committee.* AoIR.

[13] European Parliament (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* European Union: European Parliament.

[14] Federal Trade Commission (1998). *Privacy Online: A report to Congress*. United States of America.

[15] Ferguson, R. (2012). Learning analytics: drivers, developments and challenges. *International Journal of Technology Enhanced Learning, 4*, 304-31.

[16] FRA (2014). *Handbook on European data protection law. European Union Agency for Fundamental Rights.* Council of Europe. Retrieved December 10, 2014 from http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law

[17] Friedman, B. (1997). *Human values and the design of computer technology*. Cambridge, MA: Cambridge University Press.

[18] Greller, W. & Drachsler, H. (2012). Translating learning into numbers: A generic framework for learning analytics. *Educational Technology & Society, 15*, 42-57.

[19] Gotterbarn, D. (1999). How the new Software Engineering Code of Ethics affects you. *IEEE Software, 16*, 58-64.

[20] Gotterbarn, D., Miller, K. & Rogerson, S. (1997). Software Engineering Code of Ethics. *Communications of the ACM, 40*, 110-118.

[21] Government of Canada (2004). *Personal Information Protection and Electronic Documents Act*. Canada: Minister of Justice.

[22] Markham, A. & Buchanan, E. (2012). *Ethical decision-making and Internet research: Recommendations from the AoIR Ethics Working Committee (Version 2.0)*. AoIR.

[23] Johnson, L., Adams Becker, S., Estrada, V., & Freeman, A. (2014). N*MC Horizon Report: 2014 Higher Education Edition*. Austin, Texas: The New Media Consortium.

[24] Kay, D., Korn, N., & Oppenheim, C. (2012). Legal, risk and ethical aspects of analytics in higher education. *JISC CETIS Analytics Series: Vol. 1 No. 6*. Retrieved October 22, 2014 from http://publications.cetis.ac.uk/c/analytics

[25] Kobsa, A. (2007). Privacy-enhanced web personalization. In P. Brusilovski, A. Kobsa, & W. Nejdl (Eds.), *The adaptive web: Methods and strategies of web personalization* (pp. 628-670). Berlin: Springer.

[26] Levin, A. & Nicholson, M.J. (2005). Privacy law in the United States, the EU and Canada: The allure of the middle ground. *University of Ottawa Law & Technology Journal, 2,* 357-395.

[27] Long, P., & Siemens, G. (2011). Penetrating the fog. Analytics in learning and education*.* *EDUCAUSE Review, 46*, 30-40.

[28] Moore, S. L. (Ed.) (2008). Special Issue: Practical Approaches to Ethics for Colleges and Universities. *New Directions for Higher Education*, 2008(142), 1-7.

[29] Movius, L.B. & Krup, N. (2009). U.S. and EU Privacy Policy: Comparison of regulatory approaches. *International Journal of Communication, 3,* 169-178.

[30] OECD (2013a). Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data". *OECD Digital Economy Papers No. 222*. OECD Publishing.

[31] OECD (2013b). *The OECD Privacy Framework*. OECD Publishing.

[32] Pardo, A. (2014). Designing learning analytics experiences. In J.A. Larusson & B. White (eds.), *Learning analytics: From research to practice* (pp. 15-38). New York: Springer.

[33] Pardo, A. & Siemens, G. (2014). Ethical and privacy principles for learning analytics. *British Journal of Educational Technology, 45*, 438-450.

[34] PMCA (2013). *Big Data – Bedeutung, Chancen, Datenschutz* [Big Data – Meaning, Chances, Data Protection] [Press release]. Retrieved from http://www.pmca.at/pmca-impuls-16-9-2013-pressemeldung-big-data-bedeutung-chancen-datenschutz/

[35] Rodotà, S. (2009). *Data protection as a fundamental right*. In Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne,S. Nouwt (Eds.), Reinventing data protection? (pp. 77-82). Dordrecht: Springer.

[36] Scheffel, M., Drachsler, H., Stoyanov, S., & Specht, M. (2014). Quality indicators for learning analytics. *Educational Technology & Society, 17*, 117-132.

[37] Schwartz, P.M. (2011). Privacy, ethics, and analytics. *IEEE Security and Privacy, 9*, 66-69.

[38] Sclater, N. (2014, October 29). N*otes from Utrecht Workshop on Ethics and Privacy Issues in the Application of Learning Analytics* [Web log post]. Retrieved from http://analytics.jiscinvolve.org/wp/2014/10/29/

[39] Slade, S. & Prinsloo, P. (2013). Learning analytics: ethical issues and dilemmas. *American Behavioral Scientist, 57,* 1509-1528.

[40] Spiekerman, S. & Cranor, L.F. (2009). Engineering privacy. *IEEE Transactions on Software Engineering, 35,* 67-82.

[41] Stiles, R.J. (2012). Understanding and managing the risks of analytics in higher education: A guide. *EDUCAUSE*. Retrieved December 9, 2014 from http://net.educause.edu/ir/library/pdf/EPUB1201.pdf

[42] Stutzman, F. & Kramer-Duffield, J. (2010). Friends only: Examining a privacy-enhancing behavior in Facebook. In: *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2010)* (pp. 1553-15262). ACM: Atlanta.

[43] Tene, O. & Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property, 11*, 239-273.

[44] The Open University (2014, September). *Policy on ethical use of student data for learning analytics.* Milton Keynes: The Open University. Retrieved December 2, 2014 from http://www.open.ac.uk/students/charter/essential-documents/ethical-use-student-data-learning-analytics-policy

[45] The White House (2012). Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy. Washington: The White House.

[46] US Government (2004). Code of Federal Regulations. Education. Family Educational Rights and Privacy. 34 CFR Part 99. Washington: Department of Education.

[47] Van Harmelen, M. & Workman, D. (2014). *JISC CETIS Analytics Series: Vol.1 No.3, Analytics for learning and teaching*. University of Bolton, 2012. Retrieved August 19, 2014 from http://publications.cetis.ac.uk/2012/516

[48] Verbert, K, Duval, E., Klerkx, J., Govaerts, S., & Santos, J.L. (2013). Learning analytics dashboard applications. *American Behavioral Scientist, 57,* 1500-1509.

[49] Willis, J.E. (2014). Learning analytics and ethics: A framework beyond utilitarianism. *EDUCAUSE Review*. Retrieved October 28, 2014 from http://www.educause.edu/ero/article/learning-analytics-and-ethics-framework-beyond-utilitarianism

[50] Willis, J.E. & Pistilli, M.D. (2014). Ethical discourse: Guiding the future of learning analytics. *EDUCAUSE Review*. Retrieved December 1, 2014 from http://www.educause.edu/ero/article/ethical-discourse-guiding-future-learning-analytics

[51] Willis, J.E., Campbell, J.P., & Pistilli, M.D. (2013). Ethics, big data, and analytics: A model for application. *EDUCAUSE Review*. Retrieved October 28, 2014 from http://www.educause.edu/ero/article/ethics-big-data-and-analytics-model-applicat