Learning Analytics as a Service for Empowered Learners

From Data Subjects to Controllers

Nicole Gosch*

Dept. Law and IT, University of Graz,
Graz, Austria
nicole.gosch@uni-graz.at

David Andrews*

Dept. Law and IT, University of Graz,
Graz, Austria
david.andrews@uni-graz.at

Carla Barreiros*

Institute of Interactive Systems and
Data Science, Graz University of
Technology, Graz, Austria;
Know-Center GmbH, Graz, Austria
cbarreiros@know-center.com

Philipp Leitner

Dept. Educational Technology, Graz
University of Technology, Graz,
Austria
philipp.leitner@tugraz.at

Elisabeth Staudegger

Dept. Law and IT, University of Graz,
Graz, Austria
elisabeth.staudegger@uni-graz.at

Martin Ebner

Dept. Educational Technology, Graz
University of Technology, Graz,
Austria
martin.ebner@tugraz.at

Stefanie Lindstaedt

Institute of Interactive Systems and
Data Science, Graz University of
Technology, Graz, Austria;
Know-Center GmbH, Graz, Austria
lindstaedt@tugraz.at

ABSTRACT

As Learning Analytics (LA) in the higher education setting increasingly transitions from a field of research to an implemented matter of fact of the learner's experience, the demand of practical guidelines to support its development is rising. LA Policies bring together different perspectives, like the ethical and legal dimensions, into frameworks to guide the way. Usually the first time learners get in touch with LA is at the act of consenting to the LA tool. Utilising an ethical (TRUESEC) and a legal framework (GDPR), we question whether sincere consent is possible in the higher education setting. Drawing upon this premise, we then show how it might be possible to recognise the autonomy of the learner by providing LA as a service, rather than an intervention. This could indicate a paradigm shift towards the learner as empowered demander. At last, we show how this might be incorporated within the GDPR by also recognising the demand of the higher education institutions to use the learner's data at the same time. These considerations will in the future influence the development of our own LA policy: a LA criteria catalogue.

*Authors contributed equally to this research.

This work is licensed under a Creative Commons Attribution International 4.0 License.

LAK21, April 12–16, 2021, Irvine, CA, USA

© 2021 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-8935-8/21/04.

<https://doi.org/10.1145/3448139.3448186>

CCS CONCEPTS

• **Applied computing** → Education; E-learning; • **Security and privacy** → Human and societal aspects of security and privacy; Social aspects of security and privacy.

KEYWORDS

Learning Analytics, Higher Education, Ethics, Trust, GDPR, LA Policies

ACM Reference Format:

Nicole Gosch, David Andrews, Carla Barreiros, Philipp Leitner, Elisabeth Staudegger, Martin Ebner, and Stefanie Lindstaedt. 2021. Learning Analytics as a Service for Empowered Learners: From Data Subjects to Controllers. In *LAK21: 11th International Learning Analytics and Knowledge Conference (LAK21)*, April 12–16, 2021, Irvine, CA, USA. ACM, New York, NY, USA, 7 pages. <https://doi.org/10.1145/3448139.3448186>

1 INTRODUCTION

Learning Analytics (LA) collects, measures, analyses, and reports data about learners to leverage human decisions to improve learning and environments [20]. LA research is an emergent interdisciplinary field that has brought together educators, psychologists, and data scientists.

In recent years there is an increasing interest among higher education institutions (HEI) in adopting LA to enhance the quality of teaching and learning [19]. With the digital transformation, higher education institutions are collecting data as never before, e.g., administrative data, interaction data with the learning management systems and other digital learning tools. However, there are often barriers that prevent HEI to use this data effectively [3]. The challenges associated with LA implementation relate to technical, cultural, and social aspects [31]. Furthermore, Prinsloo and Slade

[25] point out that the collection, use, and dissemination of data requires an institutional policy that aligns with national and international legislative frameworks to ensure an enabling environment for LA. It is essential to establish a set of guidelines and principles to guide stakeholders (i.e., institutions, faculty, learners, researchers) and encourage ethical use of data within an educational system where power is unequally distributed among different stakeholders [27]. LA research is governed by regulations for data protection and research ethics, and the involvement of the stakeholders is based on consent to participate in the research activities. However, moving research outcomes out of the labs to be implemented as tools in the institutional LA systems, implies dealing with the constraints of the legislative framework. In the European Union (EU), this is predominantly the General Data Protection Regulation (GDPR) [13]. In its core, the GDPR seeks to empower European citizens regarding their data and aims to create a common legal frame across EU nations. GDPR key requirements regarding privacy and data protection include: freely given and informed consent of data subjects for data processing, data anonymisation to protect privacy, data breach notifications, and provisions ensuring safe international data transfer. Core principles of the GDPR, e.g. autonomy and freely given and informed consent, also are important values in other legal data protection frameworks. Several initiatives and EU projects address ethics and privacy concerning the design and implementation of LA in higher education institutions. An example of such a project is SHEILA - Supporting Higher Education to Integrate Learning Analytics [29], which proposes a policy development framework intended to assist European universities to use and safeguard the digital data about their students. We pursue a slightly different approach: Building on the rule of law and a strong European law enforcement system we go a step further and address the concept of trust in LA, by fostering just that on a multitude of ethical dimensions.

In this paper, we will first have a look at existing LA policies. These try to incorporate multi-perspective reflections into practical guidelines on how to deploy and maintain LA systems. In the centre of any LA policy are the ethical and legal frameworks. Based on ethical and legal aspects, our research aims to build a new LA policy by developing a criteria and indicators catalogue dedicated to trust in LA. The criteria and indicators should operationalise the ethical and legal dimensions by making assessable whether features of the LA technology enhances pre-defined trust relevant core areas (e.g. autonomy or privacy). The first contact point of a learner with the LA system is typically the act of consent. In the second part of this paper, we explore how trustworthy LA systems can be promoted by ethical frameworks and question whether sincere consent is possible in the higher education setting and which implications this consent could have. The third and last part of this paper deals with the most relevant legal framework in the EU, the GDPR. It outlines how a conceptual change, in the form of a paradigm shift, could create a system that allows LA processing for the benefit of learners without their consent. Furthermore, it is explored how the HEI yet could be able to use the accruing data for other purposes than for the concrete individual learner.

2 EXISTING LEARNING ANALYTICS POLICIES

Following existing approaches learning analytics depends on the constant collection of data from learners, which can create a feeling of discomfort and lead to resistance in the learners' adoption of the LA systems provided by the HEI [23]. Therefore, it is unsurprising that a critical issue for the success of LA in HEI directly relates to data privacy and ethical issues. LA policies play an essential role, as they reflect the ethical core values, the legal frame, and clarify the institution reasons to engage with LA. A LA policy should contain a set of principles that defines a course of action for LA in an institution, promoting in this way transparency and trust. Next, we present examples of projects whose outcomes brought insights and guidelines on how institutions could develop their own LA policies. The SHEILA framework was created within the context of the EU SHEILA project [29]. The framework aims to support HEI in the LA policy development process. The SHEILA framework consists of six dimensions: political context; key stakeholders; desired behaviour changes, engagement strategy; internal capacity to effect change; and monitoring and learning frameworks. These six dimensions are then decomposed in three key elements, the strategic action points, the potential challenges, and a set of guiding questions to be addressed in a LA policy [38]. The LEA's Box was a EU project [18] focused on research and development of a LA toolbox for teacher and learners. The LEA's box privacy and data protection framework was created to integrate ethical considerations and data privacy and protection, as well as to deal with these issues in the context of scientific research. Even though the framework is tailored to meet the needs of the project, it provides useful insights. The framework refers to a set of eight principles, i.e., data privacy, purpose and data ownership, consent, transparency and trust, access and control, accountability and assessment, data quality, and data management [36]. The EU project LACE – Learning Analytics Community Exchange [17] aimed to bring together research, policy and practice on the topic of LA, and covered topics such as data sharing, open LA, and implication on issues such as ethics and data privacy. The DELICATE checklist was proposed to guide the use of educational data. DELICATE stands for Determination (why LA?), Explain (be open about the goals), Legitimate (why is one allowed to have students' data?), Involve (all stakeholders), Consent (make a contract with the data subject), Anonymise (individual not retrievable), Technical (procedure to ensure privacy), External (working with external providers) [8].

Moreover, practitioners offering educational related digital services to educational institutions are or should be involved [39–41]. JISC is a not-for-profit organization for digital educational services and solutions, which deal with vendors and publishers on behalf of UK educational institutions. The JISC code of practice for learning analytics refers to a set of crucial areas for a LA policy, such as responsibility, privacy, transparency and consent. They also proposed a data protection framework, which considered specific issues related to historical data and the consent validity for alumni [7, 28].

LA policies bring together different perspectives to guide the design and implementation of LA systems. Two core parts of LA

policies are the ethical and legal frameworks. Where ethical frameworks operate on a meta-level, in the spheres of values and principles, legal frameworks try to incorporate those considerations on concrete legal bases (in the EU, mainly the GDPR [13]). The following section outlines how an ethical framework can be used to foster trust in LA and thereby question the practice of consent regarding the value of autonomy.

3 ETHICAL CONSIDERATIONS: FOSTERING TRUST AND EMPOWERING LEARNERS

Learning Analytics aims to understand and optimise the learning process of learners. The learner should, therefore be the focus of any intervention. However, plenty of ethical issues and pitfalls line the path. Problems arise in how to justify the collection of the data, how to store and protect the data and what conclusions to draw from them [32]. As analytic tools become more powerful and re-identification of the individual more probable, it is necessary to focus on privacy issues [23, 30]. Slade and Tait [35] identify ten ethical core issues of LA, including transparency, data ownership and control, accessibility of data, validity and reliability of data, institutional responsibility and obligation to act, communication, cultural values, inclusion, consent, and student agency and responsibility. Guidance for the proper usage of LA is needed to prevent LA to fail upon these obstacles. Ethical frameworks provide values and principles that one can use to build and maintain LA measures, both useful to the learner and ethically legitimate. Frameworks for information and communications technology (ICT) products in general [1, 37] and for learners specifically [8, 23, 32] are available in the literature.

3.1 Building Trustworthy Interventions

Trust and *trustworthiness* have been identified by several researchers as the fundamental issues for successful ICT [1, 8, 23, 34, 37]. Trustworthiness is an attribute of something, that can be increased by performing adequate actions. High trustworthiness leads moral subjects to trust certain things or persons. Trustworthiness can be objectively determined, and trust subjectively obtained. Regarding LA, high trustworthiness leads to more trust in LA tools. When trusting the system, learners will more likely actively participate in LA and take interventions seriously. This leads to better data and therefore, to better analysis, which, together with trusting the process, increases the learners' gain. Hence, trust is immanent to ensure an accepted and successful tool.

One framework focussing on trustworthiness as the overarching principle is the Horizon 2020 project "TRUst-Enhancing certified Solutions for Security and protection of Citizens' rights in digital Europe" [37]. Even though this framework was developed for ICT products in general, it can be applied to the learners' field. Building upon the European values and fundamental rights, six core areas of trustworthiness in an interdisciplinary approach were identified. The core areas are *transparency*, *privacy*, *anti-discrimination*, *autonomy*, *respect*, and *protection*. A criteria catalogue with corresponding manifold true-or-false indicators was developed to operationalise the core areas. To build trustworthy LA systems, one must address the core areas by meaningful actions, e.g. explaining how the LA

tools function to address transparency or implementing state-of-the-art security standards to enhance protection. When it comes to learners' consent, one specific core area is affected in particular: *autonomy*.

3.2 Can Genuine Consent Be Given Within the Higher Education Setting?

Autonomy expresses the ability of an individual to make their own uncoerced decisions by freedom of choice. When striving to build trustworthy LA technology, autonomy as a principle acts as an enabler for the learner to be recognised as a moral agent [32] and thus as somebody whose decisions should be taken seriously. Promoting autonomy on all levels results in a growth in trustworthiness. When regarding the LA process, the first choice a learner could be faced with is to give consent to participate in the LA system. Past work outlined the importance to seek informed consent with the learner, to justify the use of LA [8, 15, 26, 28, 33]. Informed consent means that the learner is informed about all the implications and rights that follow by the consent. Only then learners can decide freely. Thus, informed consent should not only be ticking just another box. However, not only has there been criticism on how informed one can actually be in an emerging complex world [6, 24], also there is the question of whether the learner is able to make an uncoerced decision in the higher education setting.

People enrol to HEI to receive higher education, resulting in wider knowledge and possibly better job prospects. Also, these institutions act as gatekeepers to higher degrees. Although a large number of HEI exist, from our perspective, the actual choice is often limited due to the personal living circumstances. So, the learner has to follow the rules of the institution and progress through the curriculum of his or her study; otherwise, he or she will not achieve a degree. This highlights an inequality of power [27], whereby the HEI has the upper hand. Consent from an individual is needed when the impulse to use LA comes from outside the individual, here the HEI. So, whenever an HEI seeks to gain consent from a learner, it actually nudges him or her to consent, just by the existing power imbalance. The asynchronous power balance undermines the autonomy of the learner and does not leave him or her a real free choice upon using the LA technology. Thus, it is at least questionable whether sincere consent can be given within the higher education setting. This makes it worth considering if there could be another way of implementing LA in the HEI setting, that primarily serves the interests of the learners.

In recent times some researchers have seen learners as mere consumers, rather than co-producers of their learning environment [4, 5, 21, 22]. The HEI seeks for consent to justify the use of LA technology, and the learner agrees, upon a questionable free choice. If the learner is the focus of the LA system, another approach should be considered. To fully commit to the autonomy and free will of the learner, a real free choice must be offered. To achieve this, we suggest a paradigm shift where the learner is seen as an empowered demander. This would result in an increased amount of autonomy and therefore trust in the intervention and most likely benefit the cause of LA systems. One way to apply this approach is to offer LA as a *service* for empowered learners. LA as a service can be described as a LA software, in whatever form HEI offers it

(e.g., dedicated LA system, LA features incorporated in learning management systems), which any learner can freely subscribe as a mean to improve their learning process. The HEI would then act as a service provider to solely focus on the learner's needs. The adoption of a LA service, thereby, must be optional and without nudging for compliance. Even though this approach safeguards the learners, it also limits the use of the collected data for other conceivable reasons by the HEI (e.g., adjust curriculum, reformulate studies program, implement measures to decrease drop-outs).

The next section views at how the GDPR could enable this approach by shifting the learner from the data subject to the data controller. Furthermore, we outline a lawful approach for HEI on how to use LA data for other legitimate purposes than the ones focussed exclusively on the learner.

4 A LAWFUL APPROACH: EMPOWERMENT BY APPLYING THE GDPR

Data protection law plays a vital role in the design of LA Services. Hoel and Chen [14] point out that data protection must be considered through the entire LA process, and that principles of "data protection by design" and "data protection by default" should be followed. The authors state in the "Requirements for LA Systems" that the gathering and measurement of data depend on the consent of the learner. However, the voluntary nature of consent is a difficult issue not only from an ethical point of view. Article 4 (11) of the GDPR [13] defines the "consent" of the data subject as "any freely given specific, informed and unequivocal expression of will in the form of a declaration or other unequivocal affirmative act by which the data subject signifies his or her consent to the processing of personal data relating to him or her". In particular, effective consent requires that the individual is free to decide and has control over the data [11, 13]. If not only the learners but also the HEI or faculty benefit from the use of an LA service, it is likely to exist an indirect compulsion for learners to participate. In connection with the voluntary nature of consent, problems may also arise if there is a power imbalance between the controller and the data subject [11, 13]. This problem is relevant when using LA in HEI settings. Whether the voluntary nature of the consent in connection with LA at HEI can be guaranteed is therefore questionable. Only the European Court of Justice can finally clarify this question.

4.1 From Data Subjects to Controllers

In order to create a LA system dedicated to learners, we consider a paradigm shift in our research, which is depicted in Figure 1. Instead of seeking uncertain and potentially invalid consent, we empower learners to remain the "masters" of their data. Learners assume the role of the controller as defined by Article 4 (7) GDPR [13], where each learner can decide on the purposes and means of processing [12]. We envision LA as a service for learners only, where learners are going to be free to decide if they want to use the LA service. In consequence, the HEI may only use this data as a pure processor, as defined by Article 4 (8) GDPR [13] based on documented instructions from the controller (= learner). The foundation of this relationship between the HEI and the learners would be a processing agreement [12]. From a data protection perspective, learners would no longer be in the role of the data subject,

which means that their rights guaranteed under data protection law to the data subject no longer apply. However, data protection law is still applicable in this context, only in a different way. The HEI as a processor would have to observe several data protection requirements [12]. In addition to general obligations, such as keeping records of processing activities, designating a data protection officer, providing technical and organisational measures and the obligation to report data protection violations, the processor is directly responsible to the controller. For example, if the HEI would like to use a sub-processor (i.e. an external person or body who processes data on behalf of the HEI), this must be approved by the learners. The most important aspect of this paradigm shift would be that the data provided by the learners may not be used for purposes other than those intended by the learners; otherwise, the HEI itself will become the controller. A system that is detached from any other purpose that the HEI may wish to pursue and is used exclusively for the benefit of the learners, a system in which the learners themselves have full control over what happens to their data, would be a desirable alternative to obtaining consent.

4.2 The Free Flow of Data: Using Personal Data Without Harming the Individual

Would this paradigm shift mean that the economic and social value of the data and the benefit to the general public is lost? Or are there ways within this approach in which this data can be used for other purposes? After all, there are legitimate concerns of HEI to use this data, for example, to improve curricula or to allow lecturers to improve their teaching. When considering this question, the second primary objective of the GDPR must not be forgotten. In addition to the protection of individuals concerning the processing of personal data, Article 1 (3) GDPR [13] provides the free movement of personal data within the Union. This second goal was included in the GDPR because the European Union has recognised the value of personal data and explicitly wants to allow its broad/extensive use without harming the individual involved. Therefore, the GDPR should be interpreted not only as a protection law but also as a sort of economic law and as a tool to make personal data economically usable while respecting the protection of the data subjects.

The critical element that combines these two interests and objectives of the GDPR in our view is the anonymisation. Anonymisation is the process by which data personal are rendered in such a manner that the data subject is not or no longer identifiable. Anonymisation enables data processing outside the provisions of data protection law. Only after the personal data from the LA system has been anonymised is it allowed to use it for any possible purpose, as stated in Recital 26 [13]. There are significant demands on anonymisation: Personal data shall only be considered anonymous or anonymised if, taking all means into account, it is reasonably unlikely that a person will be identified by the controller or by anyone else. As long as – and as soon as – the data exists in personal form, it is subject to the full protection of the GDPR [13] and may not be shared without a specific lawful basis. In addition to anonymisation in itself, an aggregation of the data, which can be a method of anonymisation, may also be considered an option to use data. Inevitably, not each aggregation leads to anonymisation, so it remains a question of the individual case whether data is still considered as personal data [2].

Figure 1: Shift of the learner from the data subject to the controller.

4.3 The Process of Anonymisation as a Processing Activity That Requires a Lawful Basis

Precisely at this point in the process, where the personal data from the LA service should be used for other purposes, it is necessary to look at this transformation: how to get from personal data to anonymous or aggregated data. Figure 2 depicts this process. The HEI, as a processor, already would have the stored data at its physical disposal. However, just because it has access to the data on the basis of the contractual relationship with the learners within the framework of the LA service does not mean that it can merely process the data for its own purposes without legal consequences. If the HEI intends to process the data for its own purposes, this would again lead to a change of role under data protection law. The HEI becomes the controller and the learners are now the data subjects, with all the implications of data protection law. Anonymised data falls outside the scope of the GDPR, but the anonymisation process itself is relevant to data protection law [2].

Anonymisation and de-identification can be a technical and organisational measure to protect personal data, especially in LA [16]. A processor may, for example, anonymise data within the processing activities carried out on behalf of the controller in order to ensure a higher level of protection when processing the data. In this case, anonymisation would be covered by the data processing agreement and does not require a separate legal basis. However, if a processor anonymises personal data in order to process them for

his own purposes, anonymisation must be regarded as a processing activity that requires a different lawful basis under Art 6 GDPR [13]. The purpose of anonymisation that is relevant under data protection law is not the removal of the personal reference itself, but the actual interest of the controller that is behind it. In order to be able to decide whether anonymisation is legally admissible, it is necessary to know the purpose of the processing. Furthermore, the technical process behind anonymisation must be disclosed. Only then is it possible to legally and ethically evaluate not only the processing but also whether anonymisation in the sense of data protection law has been achieved.

5 DISCUSSION

Drawing upon the premise that genuine consent is questionable, we develop our approach to shift the role of the learner to be the controller of her data. Thus, LA could be provided by HEI as a service to serve learners in the first place. The process of anonymisation is required to address the desire of the HEI to be able to use the collected data for extended purposes. In our research, we want to explore whether and how this approach of empowering learners by giving them the opportunity to choose LA as a service can prove itself in practice. Problems could arise in this respect, especially concerning the broad interpretation of the joint controllership of the GDPR by the European Court of Justice, which could lead to learners being joint controllers together with the HEI [9, 10]. We will therefore investigate how privacy by design and default can

Figure 2: Process of using data from Learning Analytics as a Service.

be used to create a system that gives learners the decision power about the purposes and means of processing and inspire others in the LA community to join us in thinking about this approach.

Another main focus of our research will be to find out how the data from the LA service can be used for other legitimate purposes of the HEI in accordance with data protection law. In particular, we will address the question of how anonymisation and aggregation of personal data can be achieved. Furthermore, the proper, lawful basis for the process of anonymisation, i.e. the transition from personal data to anonymised data, must be identified. This conceptual approach is intended to enable a product that, due to its privacy friendliness and trustworthiness, can be used by learners without any concern. However, LA as a service can only be successful, if there is a strong emphasis in creating a LA culture in the institution. We intent to promote LA by e.g., actively involving learners in the system design process, organizing workshops, information sessions.

We use the European GDPR to exemplify our approach, however we are convinced that the basic concept – building on genuine voluntariness – is transferable to other legal frameworks.

ACKNOWLEDGMENTS

The developed work presented here was co-funded by the Federal Ministry of Education, Science and Research, Austria, as part of the 2019 call for proposals for digital and social transformation in higher education for the project “Learning Analytics” (2021-2024, partner organisations: University of Vienna, Graz University of Technology, University of Graz).

REFERENCES

- [1] AI HLEG. 2019. Ethics Guidelines for Trustworthy AI. Retrieved October 25, 2020 from <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>
- [2] Article 29 Data Protection Working Party. 2014. Opinion 05/2014 on Anonymisation Techniques. WP 216, Adopted on 10 April 2014.
- [3] Jacqueline Bichsel. 2012. Analytics in Higher Education: Benefits, Barriers, Progress, and Recommendations. <https://doi.org/10.13140/RG.2.1.1064.6244>
- [4] Louise Bunce, Amy Baird, and Siân E. Jones. 2017. The student-as-consumer approach in higher education and its effects on academic performance. *Studies in Higher Education* 42, 11, 1958–1978. <https://doi.org/10.1080/03075079.2015.1127908>
- [5] Louise Bunce, Amy Baird, and Siân E. Jones. 2017. The student-as-consumer approach in higher education and its effects on academic performance. *Studies in Higher Education* 42, 11, 1958–1978. <https://doi.org/10.1080/03075079.2015.1127908>
- [6] Fred H. Cate and Viktor Mayer-Schönberger. 2013. Notice and consent in a world of Big Data. *International Data Privacy Law* 3, 2, 67–73. <https://doi.org/10.1093/idpl/ipt005>
- [7] Andrew N. Cormack. 2016. A Data Protection Framework for Learning Analytics. *Journal of Learning Analytics* 3, 1. <https://doi.org/10.18608/jla.2016.31.6>
- [8] Hendrik Drachsler and Wolfgang Greller. 2016. Privacy and analytics. In *Proceedings of the Sixth International Conference on Learning Analytics & Knowledge - LAK '16*. ACM Press, New York, New York, USA, 89–98. <https://doi.org/10.1145/2883851.2883893>
- [9] European Court of Justice. 2018. Facebook Fanpage. C-210/16.
- [10] European Court of Justice. 2019. Fashion ID. C-40/17.
- [11] European Data Protection Board. 2020. Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1 - Adopted on 4 May 2020.
- [12] European Data Protection Board. 2020. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 1.0, Adopted on 02 September 2020.
- [13] European Union. 2016. Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural

- persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). RL 2016/679/EU.
- [14] Tore Hoel, Dai Griffiths, and Weiqin Chen. The influence of data protection and privacy frameworks on the design of learning analytics systems. In *Proceedings of the seventh international learning analytics & knowledge conference*, 243–252.
 - [15] Kyle M. L. Jones. 2019. Learning analytics and higher education: a proposed model for establishing informed consent mechanisms to promote student privacy and autonomy. *Int J Educ Technol High Educ* 16, 1. <https://doi.org/10.1186/s41239-019-0155-0>
 - [16] Mohammad Khalil and Martin Ebner. 2016. De-Identification in Learning Analytics. *Learning Analytics* 3, 1. <https://doi.org/10.18608/jla.2016.31.8>
 - [17] LACE. Learning Analytics Community Exchange. 2020. Retrieved October 20, 2020 from <https://cordis.europa.eu/project/id/619424>
 - [18] LEA's Box. LEarning Analytics Toolbox. 2020. Retrieved October 20, 2020 from <http://kti.tugraz.at/css/projects/leas-box/>
 - [19] Philipp Leitner, Mohammad Khalil, and Martin Ebner. 2017. Learning Analytics in Higher Education—A Literature Review. In *Learning Analytics: Fundamentals, Applications, and Trends*, A. Peña-Ayala, Ed. *Studies in Systems, Decision and Control*. Springer International Publishing, Cham, 1–23. https://doi.org/10.1007/978-3-319-52977-6_1
 - [20] Phillip D. Long, George Siemens, Grainne Conole, and Dragan Gašević. 2011. *Proceedings of the 1st International Conference on Learning Analytics and Knowledge*.
 - [21] Alistair McCulloch. 2009. The student as co-producer: learning from public administration about the student–university relationship. *Studies in Higher Education* 34, 2, 171–183. <https://doi.org/10.1080/03075070802562857>
 - [22] Elizabeth Nixon, Mike Molesworth, and Richard Scullion. 2010. The marketisation of higher education. The student as consumer. Routledge, Abingdon, Oxon, New York, NY.
 - [23] Abelardo Pardo and George Siemens. 2014. Ethical and privacy principles for learning analytics. *Br J Educ Technol* 45, 3, 438–450. <https://doi.org/10.1111/bjet.12152>
 - [24] Paul Prinsloo. 2018. Student Consent in Learning Analytics. In *Learning Analytics in Higher Education*, J. Lester, Ed. Routledge, 118–139. <https://doi.org/10.4324/9780203731864-6>
 - [25] Paul Prinsloo and Sharon Slade. 2013. An evaluation of policy frameworks for addressing ethical considerations in learning analytics. In *Proceedings of the Third International Conference on Learning Analytics and Knowledge - LAK '13*. ACM Press, New York, New York, USA, 240. <https://doi.org/10.1145/2460296.2460344>
 - [26] Lynne D. Roberts, Joel A. Howell, Kristen Seaman, and David C. Gibson. 2016. Student Attitudes toward Learning Analytics in Higher Education: "The Fitbit Version of the Learning World". *Frontiers in psychology* 7, 1959. <https://doi.org/10.3389/fpsyg.2016.01959>
 - [27] Carol Robinson. 2012. Student engagement. *Jnl of Applied Research in HE* 4, 2, 94–108. <https://doi.org/10.1108/17581181211273039>
 - [28] Niall Sclater. 2016. Developing a Code of Practice for Learning Analytics. *Learning Analytics* 3, 1. <https://doi.org/10.18608/jla.2016.31.3>
 - [29] SHEILA Project. 2020. Retrieved October 20, 2020 from <https://sheilaproject.eu/>
 - [30] George Siemens. 2013. Learning Analytics. *American Behavioral Scientist* 57, 10, 1380–1400. <https://doi.org/10.1177/0002764213498851>
 - [31] George Siemens, Shane Dawson, and Grace Lynch. 2013. Improving the quality and productivity of the higher education sector. Policy and Strategy for Systems-Level Deployment of Learning Analytics. Society for Learning Analytics Research.
 - [32] Sharon Slade and Paul Prinsloo. 2013. Learning Analytics. Ethical Issues and Dilemmas. *American Behavioral Scientist* 57, 10, 1510–1529. <https://doi.org/10.1177/0002764213479366>
 - [33] Sharon Slade and Paul Prinsloo. 2014. Student perspectives on the use of their data: between intrusion, surveillance and care. Challenges for Research into Open & Distance Learning: Doing Things Better – Doing Better Things, 291–300.
 - [34] Sharon Slade, Paul Prinsloo, and Mohammad Khalil. 2019. Learning analytics at the intersections of student trust, disclosure and benefit. In *Proceedings of the 9th International Conference on Learning Analytics & Knowledge*. ACM, New York, NY, USA, 235–244. <https://doi.org/10.1145/3303772.3303796>
 - [35] Sharon Slade and Alan Tait. 2019. Global guidelines: Ethics in learning analytics. Retrieved 25.20.2020 from <https://www.icde.org/knowledge-hub/the-aim-of-the-guidelines-is-to-identify-which-core-principles-relating-to-ethics-are-core-to-all-and-where-there-is-legitimate-differentiation-due-to-separate-legal-or-more-broadly-cultural-env-5mppk>
 - [36] Christina M. Steiner, Michael D. Kickmeier-Rust, and Dietrich Albert. 2016. LEA in Private: A Privacy and Data Protection Framework for a Learning Analytics Toolbox. *Learning Analytics* 3, 1. <https://doi.org/10.18608/jla.2016.31.5>
 - [37] TRUESSEC.eu. 2018. Cybersecurity and privacy Criteria Catalogue for assurance and certification. Retrieved October 25, 2020 from <https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5be07569f&appId=PPGMS>
 - [38] Yi-Shan Tsai, Pedro M. Moreno-Marcos, Ioana Jivet, Maren Scheffel, Kairit Tamets, Kaire Kollom, and Dragan Gašević. 2018. The SHEILA Framework: Informing Institutional Strategies and Policy Processes of Learning Analytics. *Learning Analytics* 5, 3. <https://doi.org/10.18608/jla.2018.53.2>
 - [39] George Siemens. 2012. Learning analytics: envisioning a research discipline and a domain of practice. In *Proceedings of the 2nd International Conference on Learning Analytics and Knowledge (LAK '12)*. Association for Computing Machinery, New York, NY, USA, 4–8. <https://doi.org/10.1145/2330601.2330605>
 - [40] Charles Lang, Leah P. Macfadyen, Sharon Slade, Paul Prinsloo, and Niall Sclater. 2018. The complexities of developing a personal code of ethics for learning analytics practitioners: implications for institutions and the field. In *Proceedings of the 8th International Conference on Learning Analytics and Knowledge (LAK '18)*. Association for Computing Machinery, New York, NY, USA, 436–440. <https://doi.org/10.1145/3170358.3170396>
 - [41] Leah Macfadyen. 2017. What Does a Learning Analytics Practitioner Need to Know? *MLA/BLAC@LAK*.