Applicability of Information Governance for Data Privacy Compliance in the Education Sector

Danny Cheng
Information Technology Department
College of Computer Studies DLSU
danny.cheng@dlsu.edu.ph

Abstract: In 2012, Republic Act 10173 of the Republic of the Philippines otherwise known as the Data Privacy Act of 2012 was approved and published by the Philippine Congress. The regulations main purpose is to ensure free flow of information while imposing the obligation to secure and protect personal data both in the government and private sector. (Philippine Fifteenth Congress, 2012). Given the complexities of the regulation, academic institutions are having difficulties in complying as stated in (Doce & Ching, 2018). (Lomas, 2010) recommends that ISO 27001 be considered as a framework to follow which was also recommended by the NPC Privacy Toolkit (NPC, 2018) as a certification to aspire for in order to comply with the Data Privacy Act of 2012 thru the implementation of an Information Security Management Systems as it aligns with the various aspects of information management as well as the records management principles in ISO 15489. However, not all organizations would be ready to implement frameworks as discussed by (Alqatawna, 2014). In the case of ISO 27001, (Alqatawna, 2014) stated that the framework is domain agnostic and only defines requirements allowing the organization to develop its own implementation. This study presents a picture based on existing literature and a sample case of what data privacy compliance entails an academic institution highlighting the unique characteristics of the domain. The objective is to show that pivoting on Information Governance can provide a holistic approach that address the gaps identified and serve as a framework for mapping, aligning, and translating existing standards and frameworks into the education domain to eventually provide a practicable code-of-conduct for the sector to aide in its compliance efforts with the Data Privacy Act of 2012.

Key Words: information governance, data privacy compliance, data protection

1. INTRODUCTION

In 2012, the Data Privacy Act of 2012 or RA10173 (Philippine Fifteenth Congress, 2012) was passed into law in the Philippines with its subsequent implementing rules and regulations published on 2016 (NPC, 2016) and becoming mandatory after a year of probationary period in 2017. Since then, organizations and institutions have had difficulty complying due to several common factors such as understanding, resource availability, and complexity (Doce & Ching, 2018; Presbitero & Ching, 2018; Tirante & Ching, 2018) for both the private and public sector (Fabito, Ching, & Celis, 2018; Gonzales & Ching, 2018).

As part of the efforts of the National Privacy Commission to encourage and promote compliance, it has develop a privacy toolkit (NPC, 2018) that discusses the five (5) pillars of the compliance framework (see Fig. 1) and is recommending the use of industry standards such as ISO 27001 to guide organizations in their compliance journey.

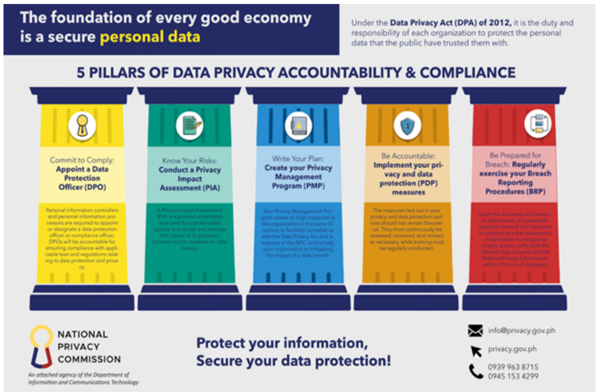

The foundation of every good economy is a secure personal data
Under the Data Privacy Act (DPA) of 2012, it is the duty and responsibility of each organization to protect the personal data that the public have trusted them with.
5 PILLARS OF DATA PRIVACY ACCOUNTABILITY & COMPLIANCE
Commit to Comply: Appoint a Data Protection Officer (DPO)
Personal information controllers and personal information processors are required to appoint or designate a data protection officer or compliance officer. DPOs will be accountable for ensuring compliance with applicable laws and regulations relating to data protection and privacy.
Know Your Risks: Conduct a Privacy Impact Assessment (PIA)
A Privacy Impact Assessment (PIA) is a process undertaken and used by a government agency to evaluate and manage the impact of its program, process and/or measure on data privacy.
Write Your Plan: Create your Privacy Management Program (PMP)
Your Privacy Management Program serves to align everyone in the organization in the same direction, to facilitate compliance with the Data Privacy Act and issuances of the NPC, and to help your organization in mitigating the impact of a data breach.
Be Accountable: Implement your privacy and data protection (PDP) measures
The measures laid out in your privacy and data protection policies should not remain theoretical. They must continuously be assessed, reviewed, and revised as necessary, while training must be regularly conducted.
Be Prepared for Breach: Regularly exercise your Breach Reporting Procedures (BRP)
Upon the discovery of a personal data breach, or reasonable suspicion thereof, it is important to conduct an initial assessment of the breach, to mitigate its impact, and to notify both the affected data subjects and the National Privacy Commission within 72 hours of discovery.
NATIONAL PRIVACY COMMISSION
An attached agency of the Department of Information and Communications Technology
Protect your information, Secure your data protection!
info@privacy.gov.ph
privacy.gov.ph
0939 963 8715
0945 153 4299

Figure 1. Five pillars of compliance framework from the National Privacy Commission (NPC, 2018)

One important pillar of compliance is the 2nd pillar which refers to the development of the Personal Data Inventory and the conduct of the Privacy Impact Assessment as it serves as the foundation for the remaining 3 pillars. This requires a clear inventory, mapping, and alignment of personal data processing with business processes and organizational goals which is complex and illustrates the importance of information and data governance in the context of an academic institution (Jim & Chang, 2018). Implementing such standards possess challenges (Alqatawna, 2014) and may need to be translated to specific domains such as the context of a university which has several differences as compared to other industries (Archuleta, 2006). The existence of academic freedom adds to the complexity of implementing standards and complying with privacy regulations (Beiter, Karran, & Appiagyei-Atua, 2016; Duncan, 2018; Frank & Melanie, 2014; Sutlieff & Chelin, 2010). Guidance specific to the education sector has been published both in the Philippines and in other countries such as the UK(DP Council Education Sector, 2020; UK Department for Education, 2018). They are either still lacking in detail or are focused on specific area of the data and processes involved in a university setting. As an alternative path to compliance and data protection, the use of information governance provides a holistic view of the data and information processed in an academic institution as well as its interactions with security and privacy stakeholders (Hagmann, 2013).

2. Related Literature

The literature review used several sources depending on the type of document to be retrieved. The literature identification process focused on (1) identifying the regulation requirements hence having the National Privacy Commission as a main source, (2) identifying industry standards on information security, data privacy, and information governance to determine current state of available documented and practiced relevant standards and to determine their applicability and gaps with respect to the study (3) published papers provide foundational basis and a view of the current state of the methodologies and solutions already presented related to the study, sample guidance's (DP Council Education Sector, 2020; UK Department for Education, 2018) were included as they were reviewed by peers in the same sector before its publication (4) samples of privacy policies in the Philippine setting to show current state of compliance and privacy policies in the UK to serve as comparison and aide in identifying gaps or improvements.

2.1 Existing Frameworks and Standards

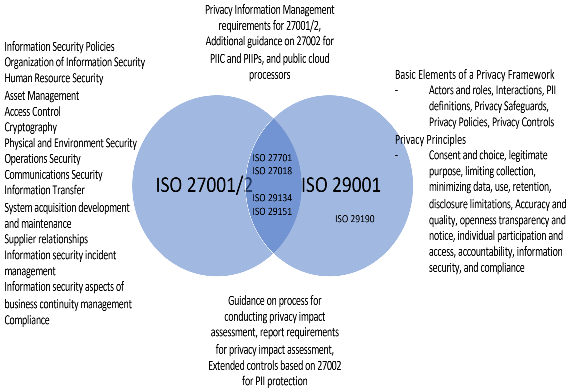

Information Security Policies
Organization of Information Security
Human Resource Security
Asset Management
Access Control
Cryptography
Physical and Environment Security
Operations Security
Communications Security
Information Transfer
System acquisition development and maintenance
Supplier relationships
Information security incident management
Information security aspects of business continuity management
Compliance
Privacy Information Management requirements for 27001/2, Additional guidance on 27002 for PIIC and PIIPs, and public cloud processors
ISO 27001/2
ISO 27701
ISO 27018
ISO 29134
ISO 29151
ISO 29001
ISO 29190
Basic Elements of a Privacy Framework
- Actors and roles, Interactions, PII definitions, Privacy Safeguards, Privacy Policies, Privacy Controls
Privacy Principles
- Consent and choice, legitimate purpose, limiting collection, minimizing data, use, retention, disclosure limitations, Accuracy and quality, openness transparency and notice, individual participation and access, accountability, information security, and compliance
Guidance on process for conducting privacy impact assessment, report requirements for privacy impact assessment, Extended controls based on 27002 for PII protection

Figure 2. Alignment and Overlaps of ISO 27001 and ISO 29001

Standards and Frameworks serve as guidance for implementing certain practices and requirements and it also serves as a common practice that people can follow to know where and how to begin. In the case of Data Privacy, several standards have been developed to address the different aspects of Data Privacy Compliance and these standards also intersect and relate to standards on information security and data protection as these are part Data Privacy Compliance. In this study, standards released by ISO relating to information security and data privacy is considered. ISO 27001/2:2013 (ISO, 2013a, 2013b) and ISO 29100:2011 (ISO, 2011) ISO 27018:2019 (ISO, 2019b), ISO 27701:2019(ISO, 2019a) ISO 29134:2017 (ISO, 2017), ISO 29151:2017 (ISO, 2017), and ISO 29190:2015ISO (2015) serves as the reference points on guidance and practices that will protect data as well as adhere to privacy principles. The main contents and relationships of the standards are shown on Fig. 2 where overlaps and dependencies are presented.

3. Methodology

3.1 Gaps in Frameworks and Standards

Alignment of the different standards and guidance based on information governance and management to comply with data privacy requirements illustrates the current state of these from information classification to information processing flow and protection. Indicative illustrations of gaps of each standard are identified and some examples are as follows:

1. ISO 27001/2:2013 (ISO, 2013a, 2013b) - Classification is required but is different from the prescription of the law. The example is based on impact or harm but the same information from the regelation can have different levels of harm.

2. ISO 27701:2019 (ISO, 2019a) - It only states the need to add PII classification. Referring to RA10173, there is ambiguity in the definition

3.2 Positioning of Information Governance

Based on the identified gaps, there is a need to provide a clearer and more practical guidance the is domain specific. Also, based on the various standards and frameworks which were initially developed for other purposes, although they are applicable to data privacy compliance, they do not fully consider or apply to it. As personal data is at the center of data privacy, the study looks at the use of Information Governance (IG) as a method of having a more cohesive and holistic approach to data privacy compliance. Information Governance programs are about minimizing information risks and costs and maximizing information value which aligns with the requirements of data privacy compliance (Smallwood, 2014). An IG model from ARMA provides a comprehensive approach that can fully align with the requirements for data privacy compliance. This addresses the limited views of existing standards and frameworks whereby their guidance focus mostly on processes. Looking at Fig. 3, it can be seen that privacy and data protection is embedded in the governance of information itself.

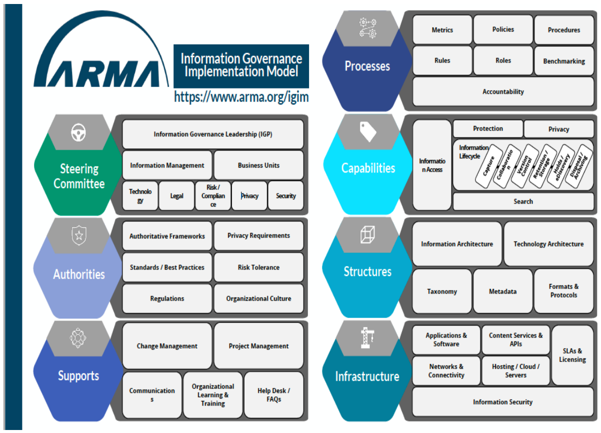
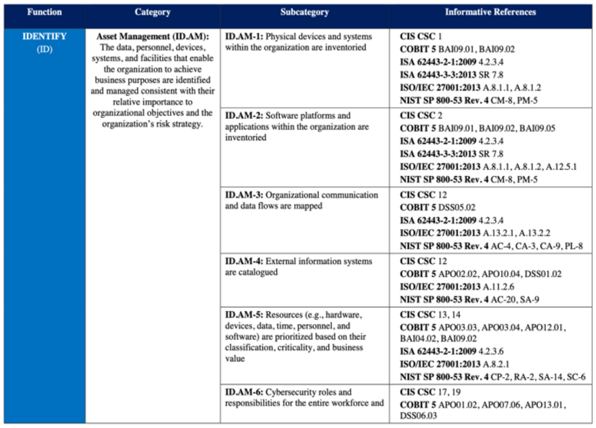


Figure 3. ARMA Information Governance (ARMA, 2020)

3.3 Mapping and aligning standards, regulations, and compliance efforts

In order for Information Governance to be a plausible approach for a holistic data privacy compliance implementation, it is shown that alignment between IG and existing data protection standards, regulations, and compliance requirements can be achieved and that one does not exclude the other but rather complements each other. As such, mapping and aligning information governance components like information taxonomy, access, and lifecycle in Fig. 3 with data protection domains like asset management as seen in Fig. 4 is used to determine a holistic view of basic industry accepted practices from an information governance perspective that can then be translated to the domain nuances of the education sector (DP Council Education Sector, 2020).



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

Figure 4. NIST Cybersecurity Framework mapping of standards and frameworks (National Institute of Standards and Technology, 2018)

3.4 Focusing on the Education Sector

Providing domain specific guidance based on data is needed to align the various requirements and standards into an implementable and practical solution. An example of which is the advisory on online learning issued by the Education Sector DP Council (DP Council Education Sector, 2020) as it focuses on the processing of personal data. This serves as an initial effort that can be expanded based on the education domain and the data flows within the domain.

4. SAMPLE USE CASE

For an educational institution to comply with the DPA, the first step is to follow the 5 pillars of compliance. At a high level of compliance, the institution can develop the needed policies and documents to comply with the law. However, the concerns arise when the details are examined and clarifications surfaces such as in the case of processing of student personal data for the purposes of admissions, enrollment, and the delivery of education. The straight forward high level compliance would be to define and collect the consent statement during admissions and enrollment, incorporate data protection measures such as encryption to the data, and prepare a breach management procedure for the data. Looking deeper into the scenario, the following are some questions and concerns that can arise:

1. Collection and processing of student personal data can have duplication within the institution where the fields of data collected may overlap and vary at the same time. Should these have their own set of consent collection or are they aligned with the existing consent collected? Is the purpose of collection visible, governed, and consistent throughout different units of the institution? Should these collection be allowed to occur? How is consent managed within the institution to reduce consent fatigue? What happens when the consent is revoked or updated? Is the consent statement consistent with the actual data flows and processing of the collected personal data? To answer these questions is that a clear and updated data flow inventory should be developed. However, if information governance does not exist, there will be inconsistent determination of the validity of the purpose, method of use, data flow, and data protection requirements of the student personal data and efforts to ensure validity would be isolated and ad-hoc that in turn creates silos of collection and processing prevalent in an educational institution that will become a consistent source of firefighting and eventually a compliance issue specially after the initial collection of the personal data.
2. Another unique point for an educational institution is the mix of data user types within the organization. Student personal data collected are not just used for the delivery of education that is in a purely academic setting, the same data is also processed in back office operations such as finance that is similar to other industries. Research utilizing the same dataset is also possible that does not only deal with statistical outputs but can also contain uses such as training datasets. There needs to be a consistent manner of orchestrating the disclosure or exchange and processing of personal data and information in general

among these different units within the educational institution.

3. Information Governance facilitates the institutionalization of data ownership and stewardship for the entire institution in order to facilitate consistent definitions of data processing policies such as approvals of processing, storage and protection, cross-border transfers, and retention policies managing and balancing compliance requirements with domain concerns such as academic freedom where freedom to choose the tool and medium of delivery may raise concerns with cross-border transfers due diligence requirements under the DPA.

5. RESULTS AND CONCLUSION

The study has illustrated the gaps of existing standards and frameworks as recommended by various industry and regulators with regards to the need for a practicable guidance or code of conduct for data privacy compliance in the education sector. The use of information governance whereby data protection and privacy compliance can be embedded would provide a comprehensive guidance focused on data and information flow for data privacy compliance instead of continuing with ad-hoc efforts and focusing solely on data protection. Much work is still needed to develop the practicable guidance or code of conduct that embeds in the day-to-day operations of an educational institution and its enterprise governance structure to fully implement and operationalize data privacy compliance. Focusing on the education domain allows for the specification to avoid being domain agnostic and provided detailed guidance on areas such as recommended data flow and processing, data protection measures, and data storage and retention details. Similar guidance can be studied and developed for other domains in the future.

6. REFERENCES

Alqatawna, J. f. (2014). The challenge of implementing information security standards in small and medium e-business enterprises. *Journal of Software Engineering and Applications, 7*, 883-890. doi:10.4236/jsea.2014.710079

Archuleta, L. S. a. K. (2006). Privacy protection and compliance in higher education: The role of the cpo. Retrieved from https://er.educause.edu/articles/2006/1/privacy-protection-and-compliance-in-higher-education-the-role-of-the-cpo

ARMA. (2020). *Information governance maturity index report 2020*. Retrieved from 2020

Beiter, K., Karran, T., & Appiagyei-Atua, K. (2016). Academic freedom and its protection in the law of european states: Measuring an international human right (european journal of comparative law and governance, 3(3), 2016, 254-345). *European Journal of Comparative Law and Governance, 3*, 254-345. doi:10.1163/22134514-00303001

Doce, L. J., & Ching, M. R. (2018). *Ra 10173 and its challenges to philippine state universities and colleges' compliance performance: The case of mindanao state university - general santos city*.

DP Council Education Sector. (2020). Advisory no. 2020-1 data privacy and online learning. Retrieved from https://www.privacy.gov.ph/wp-content/uploads/2020/10/DP-Council-Education-Sector-Advisory-No.-2020-1.pdf

Duncan, J. (2018). Criminalising academia: The protection of state information bill and academic freedom. *Communicatio, 44*(1), 107-129. doi:10.1080/02500167.2017.1415216

Fabito, B., Ching, M. R., & Celis, N. (2018). Data privacy act of 2012: A case study approach to philippine government agencies compliance. *Advanced Science Letters, 24*, 7042-7046. doi:10.1166/asl.2018.12404

Frank, B. M., & Melanie, L. W. (2014). Academic freedom in the digital age. *On the Horizon, 22*(2), 136-146. doi:10.1108/OTH-09-2013-0033

Gonzales, E., & Ching, M. R. (2018). *Performance compliance of philippine national government agency on the data privacy act of 2012: A qualitative case study*.

Hagmann, J. (2013). Information governance - beyond the buzz. *Records Management Journal, 23*. doi:10.1108/RMJ-04-2013-0008

ISO. (2011). Iso/iec 29100:2011 information technology — security techniques — privacy framework. In: (ISO) International Organization for Standardization.

ISO. (2013a). Iso/iec 27001:2013 information technology — security techniques — information security management systems —

requirements. In: (ISO) International Organization for Standardization.

ISO. (2013b). Iso/iec 27002:2013 information technology — security techniques — code of practice for information security controls. In: (ISO) International Organization for Standardization.

ISO. (2015). Iso/iec 29190:2015 information technology — security techniques — privacy capability assessment model. In: (ISO) International Organization for Standardization.

ISO. (2017). Iso/iec 29151:2017 [iso/iec 29151:2017] information technology — security techniques — code of practice for personally identifiable information protection. In: (ISO) International Organization for Standardization.

ISO. (2017). Iso/iec 29134:2017 information technology — security techniques — guidelines for privacy impact assessment. In: (ISO) International Organization for Standardization.

ISO. (2019a). Iso 27701:2019 security techniques — extension to iso/iec 27001 and iso/iec 27002 for privacy information management — requirements and guidelines. In: (ISO) International Organization for Standardization.

ISO. (2019b). Iso/iec 27018:2019 information technology — security techniques — code of practice for protection of personally identifiable information (pii) in public clouds acting as pii processors. In: (ISO) International Organization for Standardization.

Jim, C., & Chang, H.-C. (2018). *The current state of data governance in higher education.*

Lomas, E. (2010). Information governance: Information security and access within a uk context. *Records Management Journal, 20*(2), 182-198. Retrieved from https://search.proquest.com/docview/753822474?accountid=14783

http://openurl.lib.aber.ac.uk/resolver?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&sid=ProQ:ProQ%3Alisa&atitle=Information+Governance%3A+Information+Security+and+Access+within+a+UK+Context&title=Records+Management+Journal&issn=09565698&date=2010-01-01&volume=20&issue=2&spage=182&au=Lomas%2C+Elizabeth&isbn=&jtitle=Records+Management+Journal&btitle=&rft_id=info:eric/201009264&rft_id=info:doi/

http://www.emeraldinsight.com/info/journals/rmj/rmj.jsp

National Institute of Standards and Technology. (2018). Cybersecurity framework version 1.1. In: National Institute of Standards and Technology.

Implementing rules and regulations of republic act no. 10173, known as the "data privacy act of 2012", (2016).

NPC. (2018). *Npc privacy toolkit.* Retrieved from https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/3rdToolkit_0618.pdf

An act protecting individual personal information in information and communications systems in the government and the private sector, creating for this purpose a national privacy commission, and for other purposes, (2012).

Presbitero, J., & Ching, M. R. (2018). *Assessing compliance of philippine state universities to the data privacy act of 2012: The case of caraga state university.*

Smallwood, R. F. (2014). *Information governance : Concepts, strategies, and best practices* (1st edition. ed.): Hoboken, New Jersey : Wiley.

Sutlieff, L., & Chelin, J. (2010). 'An absolute prerequisite': The importance of user privacy and trust in maintaining academic freedom at the library. *Journal of Librarianship and Information Science, 42*(3), 163-177. doi:10.1177/0961000610368916

Tirante, G. A., & Ching, M. R. D. (2018). *Compliance performance of a large local company to electronic commerce act of 2000 and data privacy act of 2012: A case study approach.* Paper presented at the Proceedings of the 2nd International Conference on E-commerce, E-Business and E-Government, Hong Kong, Hong Kong. https://doi.org/10.1145/3234781.3234793

UK Department for Education. (2018). *Guidance to support schools with data protection activity, including compliance with the general data protection regulation (gdpr).* United Kingdom Retrieved from https://www.gov.uk/government/publications/data-protection-toolkit-for-schools