View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by MURAL - Maynooth University Research Archive Library

PERSONAL DATA PROTECTION
- Insights in the digital context

Introduction

This position paper presents an overview of key insights pertaining to the protection of personal data in the digital business context, as derived from pertinent academic and practitioner literature. These insights, along with insights from subject matter experts, have informed development of IVI's IT-CMF Personal Data Protection (PDP) Critical Capability.

Relevance of Personal Data Protection in the Digital Context

Data lies at the heart of an organization's digital transformation journey [1]. Through leveraging insights from the personal data of customers, the organization is enabled to make better decisions to optimize its operations, products, and services, and thereby more effectively compete, and grow its market share and revenue streams [1]. However, in the digitally connected world the organization is also increasingly challenged to protect this personal data due to the unprecedented scale of data collection, store everything practices, and the seamless flow and processing of data across various platforms and applications [1, 2, 3]. This increases potential for inappropriate or illegal data use or disclosure.

Individuals have become increasingly aware of their rights under data protection legislation - they expect organizations with which they share their data to have appropriate data protection policies and practices. Those who seek legal redress for inappropriate disclosure of their personal data are successful in approximately fifty percent of cases [4, 5]. High-profile data breaches continue to occur, leading to media coverage, legal consequences, and increased public and regulatory scrutiny [6]. Hence, effectively protecting personal data and demonstrating that the organization is a trustworthy data custodian is critical to the organization's brand equity and competitiveness [7, 8, 9].

In most jurisdictions, data protection is treated seriously. However, the developments brought about by digital transformation dictate the need for more stringent approaches to personal data protection. Research suggests that data protection controls have not kept pace with the degree to which organizations are experimenting with digital technologies and the unprecedented data volumes [1, 8][1]. Many organizations are unable to detect when or where their data systems have been breached - the FBI, banks, and credit card companies notify thousands of businesses each year that their data systems have been compromised [11].

In some jurisdictions, new regulations are enforcing stricter obligations and responsibilities on the organization to effectively protect the personal data it handles, and are imposing penalties for

[1] In an Ernst & Young survey, 37% of respondents did not have a data protection programme or only had ad hoc policies or processes in place [10]. In a further study, data loss or destruction was the top rated concern for 41% of enterprise security professionals [2].

infringement of these regulations. For example, the General Data Protection Regulation of the European Union (EU) is applicable across the EU [3, 12], and global industry standards such as the Payment Card Industry Data Security Standard [13] are mandatory when dealing with payment card data. Additional regulations continue to emerge. For example, in 2017 a proposal for a new European regulation on privacy and electronic communications was announced to keep pace with the rapid evolution of IT products and services [14].

In order to comply with requirements and avoid potentially severe legal, financial, and reputational implications of a personal data breach, many organizations need to improve their personal data protection approaches [1]. By developing the organization's personal data protection capability, the organization can reduce its exposure to the risks associated with handling personal data, while setting the foundations for its compliance with relevant legislation and enhancing its reputation.

Protecting Personal Data in the Digital Context

Data protection regulations exist to safeguard the fundamental rights of individuals to the protection of their personal data [3]. In order for organizations to be able to demonstrate compliance with such data protection regulations, it is critical that personal data protection is acknowledged and solidified as a Board level responsibility and priority [15]. Driven by the most senior executive levels, the organization may need to rethink its personal data protection strategy [1], and should reflect privacy, trust, and security as the underpinning tenets of the organization's digital strategy and the organization's brand [7, 9]. In line with the established strategies, the organization needs to develop and implement internal data protection policies and approved codes of conduct to guide its personal data protection efforts [3]. Responsibilities and accountabilities must be assigned [2, 10], and organizational resources must be deployed to ensure data protection compliance.

In some instances[2], designation of the role of the data protection officer within the organization is required to lead the organization's data protection efforts [3, 16]. This role requires collaboration across the organization, and therefore requires the support of the senior management team [16]. The data protection officer is responsible for informing stakeholders of their obligations in relation to data protection regulations, for monitoring compliance with the regulations and data protection policies, and liaising/cooperating with relevant data protection supervisory authorities/public bodies [3]. The data protection officer will also support development of a security aware culture, where heightened levels of awareness are necessary to keep pace with the types of threat actors at play and to develop new ways to act on insights gleaned from known security breaches [17]. He/She will drive awareness raising activities and training to support the interpretation of the principles of data protection regulations for those involved in personal data processing[3] operations and audits.

[2] Such instances include, for example, where data processing is performed by a public body or where data processing operations that require frequent, large-scale monitoring of data subjects or large scale processing of certain categories of personal data reflect the core activities of the organization [3].

[3] Personal data processing is 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage,

The foundation of any data protection regulation is the rights of the data subject. Hence, the organization must always be mindful of protecting these rights in its day-to-day operations. Firstly, the organization[4] is obliged to explicitly communicate to the data subject at the time of data collection the purposes for which his/her personal data is collected, the proposed processing of this data, and the associated potential risks and consequences. In addition, the data controller's contact details, the recipients of the personal data, the period for which it will be stored, and any information regarding the transfer of the personal data across multiple jurisdictions must also be clearly communicated at the outset [3]. Informed and unambiguous consent to the proposed data processing must be obtained from the data subject either through written or oral communication or by electronic means, and the organization must respect that the data subject has the right to withdraw his/her consent at any time [3, 18]. If the organization wishes to process this personal data for additional purposes, these further purposes must also be communicated and the data subject's consent is necessary prior to such processing [3].

The organization must ensure that any processing of personal data is lawful, fair, and transparent. It should only be processed in line with the specified and legitimate purposes for which it was obtained, and the data held should be adequate and limited to only that which is necessary to fulfil the specified purposes (i.e. data minimization). The organization must keep this personal data accurate and up to date, and any inaccurate personal data should be deleted or rectified without undue delay. The organization should also respect a data subject's right to request access to his/her personal data in the organization' custody and the data subject's 'right to be forgotten'. This requires the erasure of personal data when, for example, the data is no longer necessary for the purposes for which it was obtained, when data subject consent has been withdrawn, or when personal data has been unlawfully processed [3]. Where transfer of the personal data to other countries and international organizations needs to be facilitated, any lack of data protection in the foreign country should be compensated for by adequate safeguards. These may include contractual stipulations with the foreign recipient, binding corporate rules, and standard data protection clauses by a specific jurisdiction or supervisory authority including enforceable data subject rights and effective legal remedies [3, 18].

The organization should assess the likelihood and severity of risks to the rights of data subjects as a consequence of data processing. Where data processing is likely to result in a high risk to data subject rights (e.g. in instances of large scale processing of certain categories of personal data), a privacy impact assessment should be conducted. This is a systematic process to evaluate the nature and severity of the risks to data privacy across the full data lifecycle from collection to destruction, and to inform the types of measures and safeguards to be taken to mitigate those risks. The organization may also

adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction' [3].

[4] The reader should be cognizant of the terms 'data controller' and 'data processor' that are used in data protection regulations. A data controller is any legal person that either 'alone or jointly with others, determines the purposes and means of the processing of personal data'. A data processor is any legal person that 'processes personal data on behalf of the controller' [3]. The data processor processes data in line with conditions specified in a written contract agreed with the data controller.

consider the potential damage to its own reputation if data is handled inappropriately. If the severity of the risks cannot be mitigated using appropriate measures, the relevant data protection supervisory authority/public body should be consulted prior to any data processing [3, 19, 20].

It is critical that the personal data held by the organization is effectively safeguarded against unauthorized access or disclosure, unauthorized or unlawful processing, and accidental loss, destruction, or damage. Hence, the organization must implement appropriate technical and organizational measures to ensure personal data is effectively protected in alignment with regulatory and legislative requirements. In so doing, the organization should embrace the concept of data protection by design and by default, which involves considering and integrating appropriate safeguards both when determining the means by which personal data will be processed and during actual data processing itself. Developers of products, services, and applications that process personal data should take into account the right to data protection during their design and development [3, 20].

In order to ensure an appropriate level of security is afforded to personal data, as a prerequisite, the organization should establish a solid foundation of security measures to provide basic defense [10]. Security protection needs to be rebalanced from 'network centric' to 'data centric' and should specifically focus on five pillars: data center security; applications and database security; endpoints security; identity and access management (IAM); and data security [21]. Specific measures to secure and keep data confidential include, for example, strategies to anonymize/de-identify the personal data held in the organization's custody (e.g. pseudonymization or other data anonymization strategies[5]) [3, 22]. Other measures include encryption of data held centrally and on mobile devices, and the ability to wipe the data held on a mobile device via a remotely issued command in the event of its loss or theft [16]. Further measures are required to protect the availability, integrity, and resilience of processing systems and services, and to quickly restore availability and access to personal data in the event of an incident [3]. Data protection solutions should reflect an analytics-led, adaptive approach to recovery and backup that evolves with changing business needs [1]. The effectiveness of both the technical and organizational measures should be regularly tested and evaluated vis-à-vis the risks associated with data processing, and any personal data breaches should be communicated to the appropriate data protection supervisory authority/public body without undue delay [3]. In addition, the nature of any breach and recommendations to mitigate potential adverse consequences should be communicated to the data subject [3, 23] in a timely manner.

Conclusions

The effective protection of personal data is a critical factor in maintaining a positive reputation and avoiding financial and legal consequences that can threaten the organization's survival. However, personal data protection is becoming increasingly complex. As stated by Cearley et al, "*the velocity and*

[5] Pseudonymization is 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person' [3].

density of information in digital business adds new risks concerning data protection, complicated by cultural privacy issues, and in some cases, government regulations. This is made even more complicated in a world where computing is everywhere, control of those systems is incomplete, and the perimeter is almost non-existent" [24]. In the digital landscape, a rethink of the organization's data protection strategy is often required to ensure data protection controls keep pace with both rapid technological evolutions and new data protection regulations. Guided by the direction of Board-level executives, clear strategy, policies, and controls, and consistent interpretation and application of the principles of data protection regulations, the organization can build an effective personal data protection capability for the digital context.

The insights gained from evaluating the organization's personal data protection capability serve as the basis for the organization to understand 'how effective it is now' and 'what change it needs to effect'. This serves as the foundation for initiating the organization's personal data protection improvement roadmap in order to drive compliance with relevant regulations and safeguard the organization from financial and legal implications.

References

[1] C. Arend, N. Sundby, and A. Venkatraman, 'Reinventing data protection fit for digital transformation', *IDC*, 2016. [Online] Available: <https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA6-8166ENW>.

[2] Accenture, 'The state of cybersecurity and digital trust 2016 - identifying cybersecurity gaps to rethink state of the art', 2016. [Online] Available: <https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf>.

[3] European Parliament, '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', 2016. [Online] Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1489407324510&uri=CELEX:32016R0679>.

[4] J. Black, 'Developments in data security breach liability', *The Business Lawyer*, vol. 69, no. 1, pp199–207, 2013.

[5] P.N. Howard, and O. Gulyas, *Data breaches in Europe: reported breaches of compromised personal records in Europe, 2005–2014*. Budapest: Center for Media, Data and Society, Central European University, 2014. [Online] Available: <https://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/663/databreachesineurope1.pdf>.

[6] S. Pental, 'Five ways information security can help IT improve stakeholder engagement', *CEB IT Quarterly – Spotlight on business engagement*. Q2, pp30-33, 2015.

[7] Accenture, 'Accenture technology vision 2014. Every business is a digital business - from digitally disrupted to digital disrupter', 2014. [Online] Available: <http://investor.accenture.com/~/media/Files/A/Accenture-IR/events-and-presentations/Accenture-Technology-Vision-2014.pdf>.

[8] M. Brown, 'Why digital governance and data protection matters', *Computer Weekly,* 2014*.* [Online] Available: <http://www.computerweekly.com/opinion/Why-digital-governance-and-data-protection-matters>.

[9] H. LeHong, G. Alvarez, and J. Sussin, 'Ten new realities of customer engagement to account for when developing a digital strategy', *Gartner*, 2013. [Online] Available: <https://www.gartner.com/doc/2536016/new-realities-customer-engagement-account>.

[10] Ernst & Young, 'Creating trust in the digital world - EY's global information security survey 2015', 2015. [Online] Available: <http://www.ey.com/publication/vwluassets/ey-global-information-security-survey-2015/$file/ey-global-information-security-survey-2015.pdf>.

[11] S. Romanosky, D. Hoffman, and A. Acquisti, 'Empirical analysis of data breach litigation', *Journal of Empirical Legal Studies*, vol. 11, no. 1, pp74–104, 2014.

[12] European Parliament, 'Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA', 2016. [Online] Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1489407324510&uri=CELEX:32016L0680>.

[13] Payment Card Industry, 'Payment Card Industry (PCI) Data Security Standard - requirements and security assessment procedures', 2016. [Online] Available: <https://www.pcisecuritystandards.org/document_library>.

[14] European Commission, 'Proposal for a regulation on privacy and electronic communications', 2017. [Online] Available: <https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications>.

[15] International Organization for Standardization (ISO), 'ISO 38500: 2015. Information technology - Governance of IT for the organization', 2015. [Online] Available: <https://www.iso.org/standard/62816.html>.

[16] Druva, '5-step guide for GDPR compliance – a guide for constructing your planning timeline', 2016. [Online] Available: <http://pages2.druva.com/rs/307-ANG-704/images/Druva-5-Step-Guide-For-GDPR-Compliance.pdf>.

[17] Accenture, 'Accenture technology vision 2013. Every business is a digital business', 2013. [Online] Available: <https://www.accenture.com/us-en/_acnmedia/Accenture/Conversion-Assets/Microsites/Documents8/Accenture-Technology-Vision-2013.pdf>.

[18] European Union, *Handbook on European data protection law*, 2014. [Online] Available: <https://rm.coe.int/16806b294a>.

[19] Information Commissioner's Office, 'Data sharing code of practice', 2011. [Online] Available: <https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf>.

[20] Information Commissioner's Office, 'Conducting privacy impact assessments code of practice', 2014. [Online] Available: <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>.

[21] CapGemini, 'Address c-level cybersecurity issues to enable and secure digital transformation', 2016. [Online] Available: <https://www.capgemini.com/de-de/wp-content/uploads/sites/5/2017/07/1602_cybersecurity_strategic_consulting_brochure_cc_web_en_1.pdf>.

[22] Information Commissioner's Office, 'Anonymization: managing data protection risk code of practice', 2012. [Online] Available: <https://ico.org.uk/media/1061/anonymisation-code.pdf>.

[23] BakerHostetler, '2015 international compendium of data privacy laws', 2015. [Online] Available: <http://towerwall.com/wp-content/uploads/2016/02/International-Compendium-of-Data-Privacy-Laws.pdf>.

[24] D.W. Cearley, M.J. Walker, and M. Blosch, 'The top 10 strategic technology trends for 2015', *Gartner*, 2015. [Online] Available: <https://www.gartner.com/doc/2964518/top--strategic-technology-trends>.

Recommended Reading

BakerHostetler, '2015 international compendium of data privacy laws', 2015. [Online] Available: <http://towerwall.com/wp-content/uploads/2016/02/International-Compendium-of-Data-Privacy-Laws.pdf>.

J. Black, 'Developments in data security breach liability', *The Business Lawyer*, vol. 69, no. 1, pp199–207, 2013.

Council on Cybersecurity, 'Critical controls for effective cyber defense', *Gartner*, 2013. [Online] Available: <http://www.counciloncybersecurity.org/critical-controls/>.

European Parliament, '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', 2016. [Online] Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1489407324510&uri=CELEX:32016R0679>.

European Parliament, 'Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA', 2016. [Online] Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1489407324510&uri=CELEX:32016L0680>.

European Union, *Handbook on European data protection law*, 2014. [Online] Available: <https://rm.coe.int/16806b294a>.

S. Gutwirth, R. Leenes, and P. De Hert, (eds.), *Data protection on the move - current developments in ICT and privacy/data protection.* Dordrecht: Springer, 2016.

M. Hildebrandt, and K. de Vries, (eds), *Privacy, due process and the computational turn*. Oxford: Routledge, 2013.

International Organization for Standardization (ISO), 'ISO/IEC 27002: 2013. Information technology – security techniques – code of practice for information security controls', 2013. [Online] Available: <http://www.iso.org/iso/catalogue_detail?csnumber=54533>.

Joint Task Force Transformation Initiative, 'Security and privacy controls for federal information systems and organizations'. Gaithersburg, MD: National Institute of Standards and Technology, 2013. [Online] Available: <http://dx.doi.org/10.6028/NIST.SP.800-53r4>.

I. Long, *Data protection – the new rules*. Jordan Publishing, 2016.

National Institute of Standards and Technology, 'Framework for improving critical infrastructure cybersecurity', Version 1.0, 2014. [Online] Available: <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

K. Shepherdson, W. Hioe, and L. Boxall, *88 privacy breaches to beware of: practical data protection tips from real-life experiences.* Marshall Cavendish International, 2016.

Contributing Author

Dr Marian Carcary, Senior Lead Researcher, Innovation Value Institute.

About IVI

The Innovation Value Institute (IVI) is a multi-disciplinary research and education establishment co-founded by Maynooth University and Intel Corporation. IVI researches and develops management frameworks to assist business and IT executives to deliver digitally enabled business innovation. IVI is supported by a global consortium of likeminded peers drawn from a community of public and private sector organizations, academia, analysts, professional associations, independent software vendors, and professional services organizations. Together, this consortium promotes an open ecosystem of research, education, advisory support, international networking, and communities-of-practice. IVI is supported through Enterprise Ireland's and IDA's Technology Centre programme.

Contact IVI

For more information on this capability, IT-CMF and other IT management topics, or on becoming a member of IVI's international research consortium, please visit www.ivi.ie or contact us at: ivi@nuim.ie or +353 (0)1 708 6931.

Innovation Value Institute, IVI, IT Capability Maturity Framework, and IT-CMF are trademarks of the Innovation Value Institute. Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this document, and the Institute was aware of a trademark claim, the designations have been printed with initial capital letters or all in capital letters.