It's all fun and games, and some legalese: data protection implications for increasing cyber-skills of employees through games

Danaja Fabcic Povse
Centre for IT & IP Law
KU Leuven
Leuven, Belgium
danaja.fabcic@kuleuven.be

ABSTRACT

In order to combat cyber-attacks, an organisation can decide to train its employees. Improving cyber-skills of employees through educational games means their personal data will be processed and therefore it falls under the scope of the General Data Protection Regulation (GDPR). The goal of this paper is to address challenges that organisations are likely to face in practice, such as invalidity of employees' consent and over-intrusive monitoring. It argues that in order to approach training lawfully, organisations should (1) choose their external trainer with due diligence, (2) carry out a data protection impact assessment, and under certain circumstances (3) appoint a data protection officer.

CCS concepts

- Security and privacy~Social aspects of security and privacy
- Security and privacy~Privacy protections

KEYWORDS

Cyber hygiene, cyber resilience, cyber skills, GDPR, human factor, personal data of employees, privacy.

ACM Reference format:

D. Fabcic Povse. 2018. It's all fun and games, and some legalese: Data protection implications for increasing cyber-skills of employees through games. In *Proceedings of Central European Cybersecurity Conference (Ljubljana '18)*. ACM ISBN 978-1-4503-6515-4/18/11...\$15.00
<https://doi.org/10.1145/3277570.3277580>

© 2018 Copyright held by the owner/author(s). Publication rights licensed to ACM.

1 Introduction

Cyber-attacks and data breaches, which can include exploiting the human factor through social engineering, pose high economic risks. A recent report by ENISA cites the economic losses in 2014 due to cybercrime to be between €325 and €500 billion worldwide.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
CECC 2018, November 15–16, 2018, Ljubljana, Slovenia
© 2018 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-6515-4/18/11...\$15.00
<https://doi.org/10.1145/3277570.3277580>

An average individual data breach costs €3.14 million [22]. The contribution of the human factor towards cyber incidents is reported in different numbers ([26], [14]), but its high relevance to cyber-security is clear. Even though an organisation may have internal security policies in place, its employees might not comply with them. This is especially the case if employees are unaware what could be the possible consequences when they breach those policies [9]. This is a major roadblock for businesses, which must ensure security of processing, according to the General Data Protection Regulation (GDPR) [32]. Training employees and personnel to behave in a secure manner can be an important measure contributing to cyber-security.

In this paper, the author deals with the following question: how does the right to data protection apply to training employees through educational games in order to improve the employees' cyber-secure behaviour and habits in the workplace?

The goal of the paper is to focus on applicable framework of the new GDPR to cyber-hygiene according to the former's security requirements, as well as suggest a few steps towards compliance. To this end, the author will examine relevant EU legislation, case law and experts' opinions, using the doctrinal approach of legal research. It will explain the law as it stands, which in turn can inform legal practitioners working in the field [10].

First, the paper will explain how cyber hygiene is taken into account by the EU legal framework and how training employees relates to the GDPR. Discrimination in the workplace will be discussed concerning the choice of participants for training. Then, it will lay out in more detail which challenges an organisation can face while processing its employees' personal data. Finally, it will suggest some steps that organisations can take towards compliance with the GDPR.

It draws upon research previously carried out in the scope of the COMPACT project [12], which aims to strengthen the cyber-resilience of local public authorities (LPA's). In COMPACT, the employees of LPA's are trained according to the gamified approach: through playing educational games, employees will improve their cyber skills and improve their organisation's overall cyber-resilience.

However, while this paper will refer to gamified approach and discuss its implications for the right to data protection, it will not address the ethical questions of gamification per se. Nevertheless, more research into legal and ethical questions of gamification in an employment context is much warranted.

2 Data protection and cyber hygiene

The importance of cybersecurity has been recently acknowledged by the European Commission's Joint Communication on building EU-wide cybersecurity [19]. According to the European Commission, the ability to resist malicious cyber-attacks plays a very important role for protecting the economy, common prosperity and security, building the single digital market, and it also plays an essential role in protecting our democracy. It specifically mentions the need to protect personal data and establish cyber hygiene. One of the measures proposed by the Joint Communication is to improve the cyber-hygiene within an organisation. The notion of 'cyber hygiene' includes appropriate and constantly updated risk-based cyber-security programmes, including through awareness campaigns. According to the Joint Communication, cyber hygiene should be an essential part of business offers to consumers.

This is corroborated by ENISA's report on Cyber Security in organisations [22]. Cyber security culture is defined as 'the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest in people's behaviour with information technologies'. The report also explicitly notes lack of security as a reason for decrease in consumer trust.

In order to ensure internal cyber hygiene, an organisation can decide to train its staff. Privacy and data protection come into play at two points: when selecting participants for diverse educational games and when assessing the improvement of their cyber-skills throughout training.

When selecting participants for training, the organisation must be careful not to use discriminatory criteria. The principle of non-discrimination is enshrined in several important legal instruments on European Union or wider European level, such as the European Convention on Human Rights [15], the Charter of Fundamental Rights of the European Union [10] and the European Social Charter [23].

Discrimination is defined as a 'situation where an individual is disadvantaged in some way on the basis of 'one or multiple protected grounds' [21]. Discrimination regarding conditions in the workplace is interpreted widely. The notion includes 'any condition derived from the working relationship'. Training as part of work duties can be considered a condition relating to the working relationship, therefore the principle of non-discrimination must be respected when selecting participants for training. Selection criteria must be determined carefully in order not to cause discrimination based on, *inter alia*, age, ethnicity or national background, disability, sex, sexual orientation or political opinion. [21]

Under the new General Data Protection Regulation [32], organisations, which process personal data must take certain measures to ensure data protection in processing and its security, must adopt certain organisational and technical measures.

Personal data are defined in Art. 4(1) of the GDPR "as any information relating to an identified or identifiable natural person"; the identified or identifiable person is referred to as a "data subject". Employees can be data subjects like any other individual. With the latest technological advances, ICT's can be used to

process personal data for systematic monitoring of web browsing habits, location data, use of own devices at work etc. [7]

Regarding data processing requirements, an organisation can function either as a data controller or a data processor. It is an either-or situation [25], no organisation can be both data controller as well as a data processor regarding the same processing operation.

A data controller carries more de facto responsibility; under Art. 6(2) it is responsible for compliance and must be able to demonstrate it. Further, it must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR, according to Art. 24.

Nevertheless, a data processor is not exempt from the scope of the data protection framework. Among others, the processor is directly addressed by Art. 32, entitled 'Security of processing', which requires both the data controller and the data processor to adopt technical and organisational measures in order to ensure an appropriate level of security of data processing.

3 The challenges of processing employees' personal data

Educational games for employees imply their personal data will be processed, since their progress must be tracked and evaluated. However, as will be explained in this section, such processing should not be based on employees' consent.

Furthermore, an organisation must ensure that tracking its employees' progress in cyber-skills does not interfere with their private lives disproportionately. Tracking progress can lead to monitoring, which is very intrusive. In order to ensure compliant monitoring, an organisation has to assess whether such processing is necessary, whether it has valid legal basis, is it fair to the employees, transparent and proportionate to the concerns raised [2].

3.1 Lawfulness of processing

An important principle of data processing is lawfulness of processing. According to Art. 6 of the GDPR, processing is only lawful if it meets any one of the six legal bases set out in that article. These are: if the data subject – employee – has consented to processing, or if the processing is necessary for the performance of the contract, compliance with a legal obligation, to protect the data subject's or another person's vital interests, for the performance of a task carried out in the public interest or if processing is necessary for purposes of the legitimate interests, which are being pursued by the data controller or a third party.

Consent cannot be valid legal grounds.

If an organisation wishes to process data based on consent obtained from the data subject, such consent must be given freely. This means the data subject must have a genuine choice in giving or denying consent as well as exercise control over such processing. In any other scenario, consent is illusory and cannot be valid legal grounds, thus rendering processing unlawful [2]. Processing employees' data should not be based on consent, since it is unlikely to be given freely if employees are likely to face prejudice when

It's all fun and games, and some legalese: Data protection implications for increasing cyber-skills of employees through games

CECC 2018, November 15–16, 2018, Ljubljana, Slovenia

they refuse to give consent [7].¹ This is due to power dynamics and lack of power balance between an employer and an employee [2]. Therefore, alternative legal grounds must be found [7].²

Legitimate interests and compliance with a legal obligation.

Two different legal bases are potentially useful for training employees – necessary for compliance with a legal obligation or for pursuing legitimate interests of the controller. These are set out in Art. 6(1)(c) and (f), respectively. In both cases, the organization has to take into account two criteria, it must find the relevant legal obligation it is subject to or document its legitimate interests, as well as ensure that the processed data are necessary to achieve such compliance or legitimate interests, respectively.

Data processing is lawful if it is necessary for compliance with a legal obligation to which the controller is subject, according to Art. 6(1)(c). Certain EU-level legislation requires training of employees – for example, the ENISA directive [30], the new proposed Cybersecurity Act [29] and the NIS directive [18] require either cyber-training or exchange of cyber know-how; more specifically, in the law enforcement sector, both the EUROPOL and CEPOL regulations [33] [31] provide for training of police officers.

If the organization relies on the legal obligation to meet the lawfulness requirement, it must nevertheless fully inform the employee about the processing, unless an exception applies [7].

Under Art. 6(1)(f), data processing is lawful if it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

There is an exception to pursuing legitimate interests, if such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Defining legitimate interests of an organization requires a multi-level approach. Running a business falls under the protection of the right to property [23] and the employer can be held liable for acts committed by its employees, especially if the employees cause damage or commit a crime. The latter is a staple of various legal systems; for example, in the United States the employer will be vicariously liable under the *respondeat superior* doctrine [26] in the Netherlands the employer will answer under Art. 6:170 of its Civil Code [8], in Slovenia under Art. 147 and 148 of its Code of obligations [26] and in Belgium under Art. 1384 of its Civil Code [12].

Therefore, a misdeed or even mere ignorance on part of the employee can cause significant material costs to the organization, hence its interest to educate employees and improve their cyber-skills.

Nonetheless, reliance on legitimate interests is a balancing exercise. An employer must take into account the employees' rights and interests as well: for example, does keeping in-game communications private outweigh the need to peruse them when looking for poor security practices? This is a question that must be answered on a case-by-case basis, taking into account specific circumstances.

3.2 Necessity of processing

In both cases, data processing must be necessary to comply with the law or to pursue the legitimate interests of the employer. In EU law, the necessity criterion represents an essential requirement of the broader *proportionality test*. This test allows for interference with fundamental rights, such as the right to data protection.³

How to assess if a measure is necessary in the sense of above-cited provisions of the GDPR?

The necessity criterion combines a 'fact-based assessment of the effectiveness of the measure' to the pursued objective with whether such a measure is 'less intrusive compared to other options for achieving the same goal'. It is a factual test, as opposed to merely an abstract legal notion. Whether or not a measure is necessary, must be considered in the light of specific circumstances of the processing [20].

This also corresponds to the principle of *data protection by default*: the employer must make sure that, *by default*, only personal data which are *necessary for each specific purpose* of the processing are processed (Art. 25(2) of the GDPR, emphases added by the author). Therefore, when relying on other legal grounds than consent of the employee, the employer must continually assess to what extent the educational games interfere with the right to data protection and whether a less intrusive measure with an equally effective goal is available.

This has recently been confirmed by the Regional Court of Bonn in its judgment involving the WHOIS online repository [15]; if a certain piece of information is not indispensable to achieve a purpose (in this case, to keep a repository of owners of domain names), then it does not meet the necessity requirement and must not be processed.

In terms of educational gaming, this means that the game will process response times, since these are necessary in order to assess how quickly an employee reacts to a cyber-threat, but if such an assessment can be done without e.g. geo-tracking the employee's location, then it is not considered necessary and the location should not be processed.

¹ This opinion was given before GDPR entered into force, but it is corroborated in [2].

² There is an exception to employees not being able to consent lawfully: in Horizon 2020 projects, European Commission's Ethics guidance requires human participants agree to their participating in trials, regardless of GDPR rules. Therefore, in research and trial phases of research projects, employees can still validly consent to data processing, but such consent only refers to data used in

trials/research.

See https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf, retrieved on 14/06/2018.

³ See Art. 52(1) of the Charter of Fundamental Rights of the European Union.

3.3 Transparency: notification duties and the right to be informed

Employees have the right to be informed about the processing of their personal data in educational games and training and their rights as data subjects.⁴ If the legal grounds were consent, the employees would be informed at the time they gave their consent [5]. Nonetheless, even when processing is based on other legal grounds, such as necessary for compliance with another legal obligation or necessary for pursuing a controller's legitimate interests, employees must still be notified at the beginning of the processing operation. For example, this can be done before they start playing the game.

4 Towards compliance

The question is therefore how to approach the employees' training in a legally compliant manner.

The GDPR itself suggests carrying out a data protection impact assessment to improve compliance.⁵ Further, due diligence in choosing a data processor and appointing a data protection officer can also facilitate compliance.

4.1 Choosing an appropriate data processor

Why involve an external data processor? If the educational tools are provided by a third party, sometimes not all personal data will be stored on the organisation's servers. If this third party acts as a data host, it is likely to be considered a data processor [6]. Therefore, it is very important that the organisation chooses the processor with due diligence. According to Art. 28 of the GDPR, only processors that provide sufficient guarantees to comply with the GDPR can be chosen; moreover, the controller and the processor are required to conclude a written agreement on data processing, sometimes called 'processor terms'. Such an agreement is a legally binding contract. GDPR sets out its minimum content: it must legally bind the processor to the controller's instructions and set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

4.2 Data protection impact assessment

Another step is carrying out a data protection impact assessment (DPIA). Data controllers are responsible to ensure that a DPIA is carried out when the processing operation is likely to result in a high risk to the rights and freedoms of natural persons, especially if new technologies are used.⁶

When does processing result in such a high risk? A list of situations that may lead to 'high risks' was drafted by the Article 29 Working Party; the rule of thumb being that if a processing activity can lead

to two or more described risks, a data controller must carry out a DPIA. When employees improve their cyber skills through educational tools, three risks are likely to materialise: systematic monitoring, processing of sensitive personal data as defined in Article 9 of the GDPR, and processing of data of employees as a vulnerable groups [3].

Moreover, in its drafting phase, a close interaction between different departments and stakeholders is crucial. In the COMPACT project, both legal and technical partners cooperated in order to provide a clear picture of how specific risks are likely to materialise and possible solutions to them.⁷ In the end, a comprehensive questionnaire was drafted and addressed to organisations acting as data controllers in the project.

4.3 Data protection officer

Finally, a data protection officer (DPO) can be appointed. A DPO has been called 'a cornerstone of accountability' [4], namely because he or she can help facilitate compliance and act as a contact point for employees to exercise the rights they have as data subjects, for example the right to information. Not every organisation is required to appoint a DPO; an obligatory appointment is reserved for public authorities and for organisations, which deal with systematic monitoring or process sensitive personal data or personal data relating to criminal convictions and offences.⁸ A DPO must be independent from the core organisation and must not receive any instructions regarding the exercise of his or her function. He or she gives advice on data processing, monitors compliance with the GDPR, advises on the implementation of the DPIA, cooperates with the supervisory authority, and acts as the main contact point for prior consultation under Article 36. The name and contact details of the DPO can be communicated to the employees as a good practice [4].

5 Conclusion

This paper addressed the implications that increasing cybersecurity skills through games has on the right to data protection, enshrined in the General Data Protection Regulation (GDPR). It presented the most relevant provisions of the GDPR concerning processing employees' personal data. Regarding the choice of participants in educational games, it pointed out the need to respect the right to non-discrimination. Further, the paper set out some relevant challenges of processing employees' personal data, such as their inability to validly consent to such processing, and the need to inform them about the processing. Finally, it suggests some steps towards compliance including choosing a data processor with due diligence, carrying out a data protection impact assessment (DPIA) and appointing a data protection officer (DPO).

⁴ Art. 13 and 14 of the GDPR contain an exhaustive list of information that must be given to the data subject.

⁵ See especially Recital 84 of the GDPR.

⁶ Art. 35(1) of the GDPR.

⁷ In COMPACT, reports no. D1.2, D1.4, dealing with legal and ethical monitoring of the project, contain a data protection impact assessment and 'checklists', which are intended to facilitate compliance of research activities with a view to data protection.

⁸ Art. 37(1) of the GDPR.

It's all fun and games, and some legalese: Data protection implications for increasing cyber-skills of employees through games

CECC 2018, November 15–16, 2018, Ljubljana, Slovenia

ACKNOWLEDGMENTS

The research for this paper was financed by the European Commission under Horizon 2020 grant agreement no. 740712 (COMPACT - Competitive Methods to protect local Public Administration from Cyber security Threats). This paper reflects the author's view and the Commission is not responsible for any use that may be made of the information it contains.

REFERENCES

- [1] Alharthi, Kholoud K. (2016). Employer Liability for Improper Computer and Internet Use by Employees, *International Journal of Scientific & Engineering Research*, Volume 7, Issue 4, April-2016, 27-32
- [2] Article 29 Working Party, Guidelines on consent under Regulation 2016/679, WP259.01, 28 November 2017/10 April 2018
- [3] Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679, WP 248
- [4] Article 29 Working Party, Guidelines on data protection officers (DPO), WP243, 13 December 2016
- [5] Article 29 Working Party, Guidelines on transparency under Regulation 2016/679, WP260
- [6] Article 29 Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", WP 169, 16 February 2010
- [7] Article 29 Working Party, Opinion 2/2017 on data processing at work, WP249, 8 June 2017 Article 29 Working Party, Opinion 2/2017 on data processing at work, WP249, 8 June 2017.
- [8] Burgerlijk Wetboek, unofficial translation available at <http://www.dutchcivillaw.com/>
- [9] Burcu Bulgurcu et al. (2010). Information Security Policy Compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-549
- [10] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012
- [11] Chynoweth, Paul. "Legal Research." In *Advanced Research Methods in the Built Environment*, edited by Knight, Andrew and Ruddock, Les, pp. 28-38. Chichester: Blackwell, 2008
- [12] Code Civil, available at <http://www.droitbelge.be/codes.asp>
- [13] COMPACT - Competitive Methods to protect local Public Administration from Cyber security Threats, available at <https://www.compact-project.eu/en>
- [14] COMPTIA, International Trends in CyberSecurity, April 29 2016, retrieved on 09/06/2018, available at <https://www.comptia.org/resources/international-trends-in-cybersecurity>
- [15] Convention for the Protection of Human Rights and Fundamental Freedoms, full text at https://www.echr.coe.int/Documents/Convention_ENG.pdf
- [16] Court Order of Regional Court of Bonn of 30 May 2018, Docket no. 10 O 171/18, unofficial translation available at <https://www.icann.org/en/system/files/files/litigation-icann-v-epag-request-court-order-prelim-injunction-redacted-30may18-en.pdf>
- [17] Cuijpers, Collette (2007). ICT and employer-employee power dynamics: a comparative perspective of the United States' and Netherlands' workplace privacy in light of information and computer technology monitoring and positioning of employees. *J. Marshall Journal of Information Technology & Privacy Law*, Vol. 25, Issue I, 37-77
- [18] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
- [19] European Commission (2017). Joint communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Brussels
- [20] European Data Protection Supervisor (2017). Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit
- [21] European Union Agency for fundamental rights (2018). Handbook on European non-discrimination law
- [22] European Union Agency for Network and Information Security (2018). Cyber Security Culture in organisations
- [23] European Social Charter (Revised), full text at <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/163>
- [24] *Iatridis v. Greece*, 31107/96, 25/03/1999, ECHR 1999-II 75
- [25] Information Commissioner's Office (2014). Data Controller and Data Processor: what the difference is and what the governance implications are
- [26] Nowak, J. (1999). Employer Liability for Employee Online Criminal Acts, *Federal Communications Law Journal*: Vol. 51 (1999), Issue 2
- [27] Obligacijski zakonik, available at <http://pilsrs.si/Pis.web/>
- [28] Ponemon Institute, The Human Factor in Data Protection, January 2012, retrieved on 09/06/2018, available at https://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf
- [29] Proposal for a Regulation European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")
- [30] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004
- [31] Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA
- [32] 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)
- [33] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA