Title: The implications and impact of the GDPR in System Design for Data Privacy and Information Security

INF11109: Security, Audit and Compliance – Coursework 1

Matriculation Number: xxxxxxxx

August 2018

Word count: 2485

~~~~~~

Abstract

This paper seeks to discuss the importance of data privacy and how this can be embedded in corporate information systems, in the context of the introduction of the General Data Protection Regulation in May 2018. This regulation represents a major shift in how personal data is viewed as a commodity, and places ownership of that data firmly in the hands of the individual. The impact on companies collecting, storing and processing personal data will be far-reaching; existing systems will need to be examined, amended or possibly replaced altogether in order to embody the principles of privacy by design and accountability that are core elements of the GDPR.

These issues will be presented in the context of data breaches, where information security was inadequate; the paper will conclude by discussing the consequences of non-compliance with the GDPR.
~~~~~~

Introduction

The GDPR became a binding law on all 28 EU member states on 25 May 2018. It sought to replace existing data protection laws such as the Data Protection Act (1998) in the UK, harmonising those laws governing how personal data is stored, processed and transferred.

In addition to ensuring that companies comply with the new regulations, the GDPR also grants individuals (data subjects) many more rights over how their data is stored, used or passed on. It also includes a "right to be forgotten", for example having search results removed from Google, if that would be damaging to an individual's reputation. Data subjects must be able to see the data that is held about them, and have it amended if required.

Non-compliance with the GDPR can now lead to major fines and sanctions, such as legal proceedings and the rights of data subjects to sue for damages. This is, of course, over and above the damage to the company's reputation and standing.

The GDPR also applies to companies based outwith the EU, but who process data pertaining to EU citizens. The result of this will be that many large, significant corporations worldwide will be impacted by the GDPR, and it is paramount that the significance of how the new regulations will affect them, is sufficiently understood.

Challenges

The major challenge in this paper is identifying useful and relevant material regarding the GDPR. The introduction of this law represents a major shift in the legal approach to data ownership and protection, and as such, many businesses are faced with making major changes to their information systems, policies and recording systems. A recent study found that only 54% of UK companies surveyed have plans in place to deal with a data breach (Steven and Longstaff 2017). Most companies seem to be aware that this must change when the GDPR is implemented, and there is an overwhelming body of information available to inform and assist. Just about every law firm, computer-related business and technical author, both professional and amateur, has produced a guide, report, e-book or infographic, offering their "take" on how the GDPR will affect us all after 25 May 2018. The quality, however, is variable and it may be a challenge for companies to separate the wheat from the chaff.

Research Approach

As identified above, there is a wealth of information out there and some items are more relevant, accurate and valuable than others. Much of this paper deals with points of law and rather than rely on the interpretation of others, the actual GDPR itself has been consulted wherever possible, along with other publications and papers produced by the European Parliament. Wherever a legal opinion was required, articles produced by reputable, established, international law firms were sourced. Likewise, where technical viewpoints were involved, articles and papers from established names in the computer and cyber-security industries were used. Some opinion pieces, blogs and editorials were considered, but then rejected as lacking in accuracy or otherwise being of poor quality. The earliest source used was from 2004, which may seem quite old, but the issue of data outsourcing first began to appear then and it is still relevant today; the majority of sources used are no older than 3 – 4 years.

Security and Privacy surrounding the GDPR

Privacy and Data protection

The advent of personal computers from the beginning of the 1980s and the popular availability of the Internet from the 1990s has led to an increasingly globalised and computer-connected world. Some sources predict that in only a few years, the High Street will no longer exist as we know it, due to the rise in popularity of online retailers such as EBay and Amazon (Griffits 2018).

This spectacular rise in online retail and the use of smart devices relies on individuals supplying data, and data is a valuable commodity. It is collected, stored and processed by the companies who require it; unfortunately, it can also be sold on, leaked, corrupted or stolen. Legal requirements in various countries are concerned with the protection that companies offer to the data they hold on individuals. Increasingly, data is viewed as the property of the individual, and the shift in focus in recent years has been to grant that individual much more say over how their data is used.

At the point of introduction of the General Data Protection Regulation (GDPR), there were 28 member states in the European Union, each with their own set of Data Protection regulations. These varied quite considerably between states, and one of the main aims of the GDPR was to harmonise data protection regulations between them. In addition, the GDPR introduced many more rights to the persons supplying the data (data subjects), including a right to privacy so that their data would not be subject to misuse.

Privacy by Design

Privacy by Design is a key concept embodied into the GDPR. It examines the design of data-processing and information systems and aims to incorporate privacy for the individual into the fundamental designs, rather than simply relying on regulations and sanctions for when things go wrong.

Seven foundational Principles of Privacy by Design have been identified (Cavoukian 2017), and should be incorporated from the ground up in any system that processes personal data. In summary, these are -

1. Privacy by Design must work in a proactive, rather than a reactive, manner, i.e. – it must identify potential risks and eliminate them before a data breach occurs, rather than merely reacting after the event
2. Privacy should be the default setting, where options are given
3. Privacy should be embedded in the system design
4. The functionality of the system should not be impaired, but must maintain both privacy and security
5. Security must be applied throughout the whole lifecycle of the system
6. Data retention and processing must be visible and transparent
7. The users' interests and needs must always be considered in the design and development of any system

Privacy by Design is codified in Article 25 of the GDPR and as such, applies to all systems that collect, store and process data that belongs to any EU or UK data subject (Eur-lex.europa.eu. 2016). As new systems are designed for corporate entities, these principles can be embedded within them, thus ensuring that data processors and controllers can comply with the new regulations. Where this may be more problematic is applying these principles to legacy systems; it may not be desirable or even workable to merely superimpose Privacy-Enhancing Technologies (PETs) on top of existing, outdated methods (Danizis et al 2014).

Scope of the GDPR

The GDPR applies to any data pertaining to natural persons, and protects their rights to privacy of that data (it does not apply to legal "persons", such as limited liability companies). Data may be part of a database of records (for example medical records, credit card information, voter registrations, Government databases such as DVLA). As well as digital records, manual records are also included; any sort of filing system comes under the scope of Article 2(1) of the GDPR. It makes no difference whether the data processing is digital or manual (Eur-lex.europa.eu. 2016).

There are some exceptions to the scope of the GDPR. Where the data processing relates to matters of national security, humanitarian crises or for some specific political purposes, then the GDPR does not apply. Criminal justice cases are not bound by the GDPR either, but by the Police and Criminal Justice Data Protection Directive (Guild 2015).

Companies have to be aware of data processing where the data is possibly transferred outwith the EU. In recent years it has been common practice to outsource large data-processing tasks, particularly the migration of paper-based records to digital format. If there are many records to process, it becomes tempting for cash-strapped companies to pursue the cheapest option, not necessarily considering either the security of the data or the quality of the processing (Dečman 2007, Lum 2004).

The GDPR applies not only to data processing that occurs in the EU; it applies to the data pertaining to any individual who is resident in the EU, whether the actual processor is in the EU or elsewhere. This will have massive implications for international companies such as Facebook or Google, who use data collected from their subscribers to provide targeted advertising through services such as DoubleClick (Barnett 2018). Facebook in particular has come under much criticism in the past for their poor handling of collected data, a recent example being the sharing of Facebook-harvested data with the political consultancy firm Cambridge Analytica (BBC World News 2018). This sharing of personal information would now be illegal under the GDPR, and the companies concerned subject to large fines and other sanctions.

Requirements for companies

Companies must now be able to demonstrate that their data processing systems comply with the principles described in GDPR Articles 5(i) and 5(ii). Some examples of proving compliance are –

1. A clear and comprehensive data-privacy policy, that is available to view for everyone involved, and sets out full details of how data will be processed, including any legal aspects, any security measures in place for international data transfers, and the length of time that data will be retained
2. The appointment of a Data Protection Officer (DPO), and training to ensure that all staff understand their obligations under the GDPR
3. Incorporation of the main principles of the GDPR into their corporate Code of Conduct
4. Ensuring that full, accurate and transparent records are available of all data processing activities
5. Making information available advising the data subjects of their rights, and how they can access any data held about them
6. Data Protection Impact Assessments, for high-risk processing of data

One example of implementation may be that of an existing company website, which now incorporates an "accept" button or box to tick; this lets the reader review their rights under the GDPR and agree with them, before they are allowed to proceed to the rest of the site.

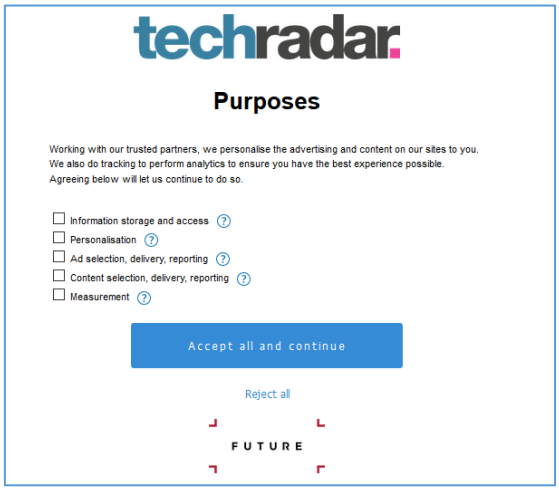

Figure 1 – users landing on a website for the first time are required to state how they will permit their data to be used. Example from https://www.techradar.com/uk/news

Article 24 of the GDPR specifically requires companies to implement 'appropriate technical and organisational measures' to demonstrate compliance. As well as the documentation and internal policy measures mentioned above, the data itself may require encryption or pseudo-anonymization. Systems must be proven reliable and resilient; in the event of system failure, data backups must be available. It goes without saying that the backups should be tested at regular intervals, to ensure that they are still uncorrupted and useable (Davidson 2018).

Data controllers may refer to the CIA Triad diagram to help ensure that their data confidentiality, integrity and availability are always maintained.

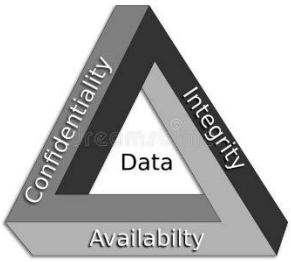

Figure 2 – the CIA data security triad. Copyright-free image from dreamstime.com

Recording and Security

Written records must be kept of all data processing according to Article 30 of the GDPR (some small companies with <250 employees many be exempt, provided this does not interfere with the data subjects' rights). These records must include the contact details of the Data Controller and the purposes of the data processing. If the data is to be transferred outside the EU, these details should also be recorded. In all cases, the lifespan of the data must also be specified.

For many companies, these obligations will be much greater than before and new technical and security measures would require to be implemented. This may well lead to additional costs for the data processing and storage, as well as potential changes in the way that the data has previously been processed, if this is deemed to be insecure.

What if the worst should happen?

The consequences for companies of a data breach are severe and far-reaching. In 2011, the Sony PlayStation Network was taken offline for 23 days, because of a "criminal intrusion"; it later transpired that some 77 million accounts containing personal data had been compromised. This was one of the largest data breaches in history, and Sony estimated that the downtime alone had cost them approximately $171 million (Hachman 2018). In an attempt to restore customer confidence, they offered some of their games for free (Caplin 2011); they were also fined £1/4 million by the UK Information Commissioner's Office, partly because they waited for over a week until the breach was reported. In addition, their insurers, Zurich American, took legal action to have themselves released from any indemnity resulting from the data breach (Bonner 2012).

It is therefore in the company's interests to ensure that data is secured and protected, as the penalties under the GDPR are even greater now than those faced by Sony. Such a breach would now have to be reported to the relevant authorities within 72 hours, accompanied by an explanation of the nature of the breach and details of the records compromised (DPWP 2017). The data subjects must also be informed as soon as practically possible, unless there are special extenuating circumstances.

Where data controllers and processors do not comply with the GDPR, there are harsh penalties; they become liable for fines of up to 10 or 20 million euro, or 2 or 4% of their previous year's worldwide turnover (not profit). Data subjects also have the right to sue for compensation for any damages they may have suffered. As Sony's global turnover in 2017 was approximately $77 billion (Statista 2018), this makes a £250,000 fine look pretty insignificant!

Conclusions

This paper has drawn on a number of articles, reports, legal documents, white papers and academic papers that focus on the GDPR and its implications for data privacy and information security. The impact of the GDPR on many companies, in terms of their operation and the financial implications, remains to be seen, but this paper may come as a wake-up call to company executives who are unprepared and consequently, have left their respective businesses in danger of non-compliance. The key themes, set out in non-technical language, include building data privacy into system design, accountability, and the consequences of data breaches where systems are insecure.

References

Anon. (2018). Sony revenue 2007-2017 | Statistic. [online] Statista. Available at: https://www.statista.com/statistics/279269/total-revenue-of-sony-since-2008/ [Accessed 31 Jul. 2018].

Barnett, M. et al, (2018). How GDPR will impact Facebook, Google and online advertising. [online] Marketing Week. Available at: https://www.marketingweek.com/2018/05/09/gdpr-impact-facebook-google-online-advertising/?ct_5b60981913ca3=5b60981913d45 [Accessed 31 Jul. 2018].

BBC News. (2018). Facebook scandal 'hit 87 million users'. [online] Available at: https://www.bbc.com/news/technology-43649018 [Accessed 31 Jul. 2018].

Bonner, L. (2012). Cyber Risk : How the 2011 Sony Data Breach and the Need for Cyber Risk Insurance Policies Should Direct the Federal Response to Rising Data Breaches. [online] Openscholarship.wustl.edu. Available at: https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1581&context=law_journal_law_policy [Accessed 31 Jul. 2018].

Caplin, N. (2011). Details Of The Welcome Back Programme For SCEE Users. [online] PlayStation.Blog.Europe. Available at: https://blog.eu.playstation.com/2011/05/16/details-of-the-welcome-back-programme-for-scee-users-2/ [Accessed 31 Jul. 2018].

Cavoukian, A. (2017). Privacy by Design, The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices. [online] Iab.org. Available at: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf [Accessed 31 Jul. 2018].

Davidson, B. (2018*).* Getting to know the General Data Protection Regulation, Part 7 - Accountability Principles = More Paperwork - Privacy, Security and Information Law Fieldfisher. [online] Privacylawblog.fieldfisher.com. Available at: https://privacylawblog.fieldfisher.com/2016/getting-to-know-the-general-data-protection-regulation-part-7-accountability-principles-more-paperwork [Accessed 31 Jul. 2018].

Data Protection Working Party (2017). Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679. Brussels, Belgium: Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, p.5 et seq.

Dečman, M. (2007) "Long term Digital Archiving - Outsourcing or Doing it." The Electronic Journal of e-Government Volume 5 Issue 2, pp 135 - 144, available online at www.ejeg.com

Eur-lex.europa.eu. (2016). Official Journal of the European Union, L119/48 [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN#page=48 [Accessed 31 Jul. 2018].

The European Union Agency for Network and Information Security (2014). Privacy and Data Protection by Design – from policy to engineering. Heraklion, Greece: ENISA, p.56.

Griffits, P. (2018). How Amazon is destroying the British high street | Coffee House. [online] Coffee House. Available at: https://blogs.spectator.co.uk/2018/05/how-amazon-is-destroying-the-british-high-street/ [Accessed 31 Jul. 2018].

Guild, E. (2015). The EU Data Protection Directive on Police and Criminal Justice Cooperation – BREXIT Impacts for the UK? | Brexit blog. [online] Kingsleynapley.co.uk. Available at: https://www.kingsleynapley.co.uk/insights/blogs/brexit-blog/the-eu-data-protection-directive-on-police-and-criminal-justice-cooperation-brexit-impacts-for-the-uk [Accessed 31 Jul. 2018].

Hachman, M. (2011). PlayStation Hack to Cost Sony $171M; Quake Costs Far Higher. [online] PCMag UK. Available at: https://uk.pcmag.com/news/106573/playstation-hack-to-cost-sony-171m-quake-costs-far-higher [Accessed 31 Jul. 2018].

Lum, M. (2004). Offshore Outsourcing and Information Confidentiality Foreign Practices and US Laws: Trends, Incidents, and Possible Solutions. [online] Sans.org. Available at: https://www.sans.org/reading-room/whitepapers/legal/offshore-outsourcing-information-confidentiality-1438 [Accessed 31 Jul. 2018].

Steven, J. and Longstaff, S. (2017). Data breach response: readiness vs the reality. [ebook] Nottingham, England: Experian, p.5. Available at: http://www.experian.co.uk/databreach [Accessed 1 Aug. 2018].

Paper /Source	Aspects covered	Approach	Key themes and findings
Griffits (2018)	Rise in use of online data	Editorial piece in established political/current affairs magazine – sets context from implications of GDPR	Impact of online retail in our everyday lives
Cavoukian (2017)	Privacy by Design enshrined in the GDPR	Paper written by the Information Commissioner of Canada, principles enshrined in the GDPR	What data subjects and processors can expect from the GDPR
Danezis et al (2014)	Specific examples of implementation of the GDPR	Report by ENISA regarding privacy and data protection, including examples of system design in context of the GDPR	Protection and encryption of data, embedding the protection and privacy of data into design systems
Eur-lex.europa.eu. (2016)	Privacy by Design, draft of GDPR	Official EU directive for incorporation in the GDPR	Describes privacy by design and it's application to all information systems
Guild (2015)	Impact of the GDPR and EU Police & Criminal Justice Directive on UK subjects	Article written by partner in large, recognised firm of international lawyers dealing specifically with user data in international context	Describes criminal cases and how they will be impacted a) by the GDPR/DPDPCJC in the context of Brexit
Dečman (2007)	Potential consequences of outsourcing data processing	Academic paper by Dr Mitja Dečman University of Ljubljana, Slovenia.	Researches and discusses the needs, volume, requirements and potential drawbacks of outsourcing data-processing from Slovenia to other countries
BBC (2018)	Data sharing which would now be illegal under the GDPR	Website of the BBC, commonly regarded as reliable, provides verifiable facts	Discusses the sharing of users data and the potential impact on the US Presidential elections, amongst other things
Barnett (2018)	Impact of GDPR on companies outside the EU	Article in established trade journal regarding marketing	Discusses the impact of using data to supply targeted adverts embedded in webpages
Lum (2004)	Data processing outsourcing	Article from SANS institute reading room, leading authority on cyber security	Discusses the implications of outsourcing, also examines the risks and cites real-world incidents
Davidson (2018*)*	Accountability principles of GDPR	Article by partner in large International law firm	Discusses the impact of accountability in the context of the GDPR for firms with international markets
Hachman (2011)	Impact of serious data breach	Article in established computer trade magazing	Discusses the Sony Playstation hack and the consequences for both customers and firm

Caplin (2011)	Financial consequences for Sony as result of breach	Blog post by Sony (Europe)Technical Officer	Demonstrates one of the consequences of major data breach
Bonner (2012)	Other consequences for Sony as result of breach	Academic paper from Washington University Journal of Law & Policy	Investigates impact of data breaches on liability insurance
DPWP (2017)	Financial penalties for breach of GDPR	Guidelines published by the European Parliament	Lays out the financial penalties that may be imposed on companies in breach of the GDPR
Anon (2018)	Statistics	Website of collated statistics for turnover of major corporations worldwide	Shows annual turnover for Sony and ergo, potential new maximum fine under GDPR
Steven and Longstaff (2017)	Company readiness to respond to data breaches	White paper produced by major credit and financial company	Contains surveys regarding the readiness of UK companies to comply with GDPR and deal with data breaches