The EU GDPR

An evolution or revolution in privacy?

Prepared for Innopsis and sponsored by The Common Framework.

Written by Des Ward (Information Director, The Common Framework and Information Governance Director, Innopsis)

Published – 11th January 2018

Executive summary

The European Union (EU) General Data Protection Regulation (GDPR)[1] is entering the end of its two-year implementation period, and guidance on specific areas is still being published.

This guidance will not be a surprise to those organisations who have mature information governance and security regimes which take current legal and regulatory requirements into account.

However, it will provide much needed clarity to those organisations who have ran tightly-scoped compliance regimes which have been compromised by the recent advances in disruptive technologies (which have a tendency to not respect compliance boundaries).

The mounting deficit between the compliance approaches and reality is being brought into sharp focus from not only the guidance, but the U.K. implementation of the GDPR, through the Data Protection Bill making its way through parliament.

Recent cases against Morrisons supermarket and the Carphone Warehouse show that the legal framework is not restricted solely to data protection and that controls must apply throughout the organisation respectively.

This document attempts to present the challenges to suppliers from not only the GDPR but also the current guidance from the Article 29 Working Party, and the current wide legal context of laws affecting information. Whilst written for suppliers, it is likely that it will provide benefit for anyone who is either planning or undertaking compliance programmes for the GDPR.

Understanding the challenges allows organisations affected by the GDPR to quantify the business benefit resulting from showing compliance.

[1] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Introduction

The European Union (EU) General Data Protection Regulation (GDPR) has made the press a lot over the past year, and this will intensify at the end of the two-year implementation period that started after it came into force in May 2016. The latter part of the preceding sentence may come as a surprise to you, but rest assured that the GDPR came into force a month after publication in April 2016. It merely becomes enforced after a two-year implementation period which ends on the 25th May 2018.

There are a lot of myths surrounding the GDPR and an even greater misunderstanding of the changing landscape for suppliers and their customers. This article will cover a lot of these areas to allow you to prepare for the 25th May 2018 deadline.

"The GDPR has been described by Information Commissioner Elizabeth Denham as 'an evolution, not a revolution' in data protection law, and this is broadly true; but in one area it will fundamentally change. Until now, effectively all responsibility and liability for compliance has rested with the data controller, but GDPR introduces the concept of 'processor liability'.

Now, processors are also potentially on the hook for regulatory action, and likely to have data subjects enforcing rights directly against them; the problem for those negotiating contracts is that no one quite knows how this will pan out.

One thing that seems certain to happen is that the negotiating tactics of processors will harden - previously, they might have been happy for the controller to specify details which now they will want to pore over. Controllers and processors alike will want to make sure they have their best commercial people on board during negotiation."

Jon Baines, Chair of NADPO (the National Association of Data Protection Officers)

The regulations cover all personal data, not just personally identifiable information

You will often hear commentators (and indeed providers of GDPR compliance services) talk about Personally Identifiable Information (PII) in the same context as the GDPR. While many people are simply using this term as short-hand for personal data, it can actually cause issues when scoping your compliance activity.

PII is an American term that concerns itself with a limited set of personal data that can directly identify someone (name, address, date of birth etc.), whereas Article 4 (and Recital 26) of the GDPR contains a far wider definition that includes the majority of metadata and ancillary information (e.g. networking details, cookies etc.) commonly found during digital transactions that could be linked to an identified or identifiable natural person.

You may well think that the distinction between PII and personal data is splitting hairs, but if you ask a supplier about PII and relevant scope you may well get a different answer than if you discuss personal data. Always make sure that you use the term personal data to avoid confusion.

Using encryption/pseudonymisation isn't the answer (on its own)

Whilst pseudonymisation and encryption is commonly mooted as a means to reduce the scope where the requirements of the GDPR apply, care should be made to refer to not only Recital 26 (discussing the effectiveness of encryption and pseudonymisation in reducing the linkage to personal data), but also the guidance on breach notification[2] from the Article 29 Working Party[3] (which discussed how flaws in the implementation or current/future weaknesses within it could result in a reclassification of encrypted personal data, and require notification of a breach even though it happened in the past).

As discussed later on in this article, it is important that you do not rely on the mere presence of a control, but look at the risk being managed and the control's performance.

Further reference should be made to the Article 29 Working Party guidance on data portability[4], which provides further clarity on the need for end-to-end encryption and the access control requirements when transferring personal data.

Is it important to ensure that you have documented not only the requirements for the encryption/pseudonymisation of personal data, but the risks that led for that control to be adopted and how you know it remains effective.

It's not a security thing, it's a governance thing

You will hear many commentators talk about the GDPR as a security exercise, yet only 3% of the GDPR is concerned with information security as we understand it today (and even those are only at the lower end of the fine regime).

Looking through Articles 25 and 32 will tell you that you have to understand the risks for not only for confidentiality, integrity, availability and resilience, but also the risks to the rights and freedoms that you face for your services and systems that process personal data and why your current activities address those challenges.

Again, the Article 29 Working Party guidance on breach notification discusses how breaches are not constrained to those of the confidentiality of personal data, but the loss of integrity/availability of it where that loss can cause an impact to a data subject.

Beyond this, there are a range of requirements within the GDPR that are far beyond information security and relate more to the ability to provide evidence that you have been fair and transparent about the processing that you have undertaken.

The Article 29 Working Party guidance on consent[5] and transparency[6] confirms that controllers and processors are to identify the purposes of processing and who processes it, generic statements such as *"processed in accordance with Data Protection requirements"*

---

[2] https://ec.europa.eu/newsroom/document.cfm?doc_id=47741
[3] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
[4] http://ec.europa.eu/newsroom/document.cfm?doc_id=44099
[5] http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849
[6] http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

and *"shared with trusted third parties"* are no longer acceptable, you must identify to both yourselves and your customers why you need to process personal data.

The areas of privacy governance, and information management are those that attract the higher rate of fines available. Searching for the term 'compliance' throughout the GDPR keeps reinforcing that the only compliance applicable is compliance with the entire requirements of the GDPR.

> *With this guidance, it is crucial to ensure that you are not just able to protect the information, but also to provide evidence that it is acquired, processed and managed in line with the GDPR requirements, remains accurate and can be retrieved when required.*

It is crucial to remember that there is not a single service, product or supplier that can (by themselves) allow you show compliance with the requirements of the GDPR, this is something that requires controllers to manage throughout the lifecycle of processing personal data. The only real way to show compliance is through effective risk and governance.

Manage risks and opportunities

We often talk about risk management, and indeed it's mentioned through the GDPR, but the approaches to risk management are often fragmented and contradictory.

If we look at the definition of risk management that the UK Government delivered through its Orange Book on Risk Management[7], we see that *"risk is defined as this uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. The risk has to be assessed in respect of the combination of the likelihood of something happening, and the impact which arises if it does actually happen"*.

So, we can view risk as being an aggregation of the:

- threats that occur because of the environment that the organisation works in (i.e. the locations, business processes and services that are used to capture, process and store information)
- the impacts that result in failures of protection, accuracy and access relating assets that process personal data (i.e. the obligations)
- vulnerabilities that allow threats to cause impacts as a result of processing personal data (i.e. the requirements for information and service assurance to mitigate the threats)

Managing the risks in this manner allow us to not only concentrate on the negative impacts from failing to comply with the GDPR, but also achieve positive outcomes from the use of personal data.

> *"If staff aren't given adequate tools to deliver in their job, then you run the risk of them going out and finding their own alternatives. If this happens then employers have no visibility or control over what is being used" – GDS*

[7] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

Consent is the last resort to determining lawful processing, not the first

When people discuss the lawfulness of processing, they often discuss the requirement for consent. Whilst consent can be a useful tool to determine if you are able to process personal data, it should be considered as the last resort when determining why you are processing information. The reason for this is withdrawal of consent may prevent you from undertaking your legal obligations (e.g. for responding to lawful enforcement, managing financial transactions etc.) or monitoring the security of systems (something that is already stated as an example of appropriate technical and organisational security within the Article 29 Working Party guidance).

Consent is also unlikely to be something that will be relied upon when a data subject has no choice but to use your service/system (and indeed the Article 29 Working Party guidance on data processing at work[8] has already stated that consent in that context is not something that is likely to be relied upon).

An exception to this may be where explicit consent is required for special categories of personal data. Special categories of personal data are defined within Article 9 and the conditions that could allow lawful processing of this type of personal data is detailed within Article 9.2.

The recent Article 29 Working Party guidance on consent should be consulted to ensure that any consent you capture is valid, especially in contracts (or terms and conditions).

> *"The two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred." – Article 29 Working Party*

You need to clear on the purposes for processing personal data; you must ensure that consent (if required) is captured for each purpose, prior to processing. Consent must be distinct and not obtained just by agreeing to a contract/terms and conditions.

> *You should take steps to ensure that your privacy notice clearly explains what processing is required and the rights that data subjects have. The ICO provides further guidance[9] on this subject.*

Data processors cannot state they were simply 'following orders'

The GDPR formalises the compliance requirements of suppliers that process personal data as data processors on behalf of data controllers. It could be argued that a breach of the Data Protection Act would likely result in the supplier being implicated anyway, but it was the controller themselves who were directly responsible.

Data controllers must provide written instructions on how processing must be conducted, and only use processors that can provide sufficient guarantees that the GDPR shall be

[8] http://ec.europa.eu/newsroom/document.cfm?doc_id=45631
[9] https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

complied with, otherwise they are still fully liable for any issues arising from the data processor's activities.

Conversely, data processors have an obligation under Article 28.3(h) of the GDPR to inform controllers where they feel that an instruction infringes the GDPR, and inform the controller when they further outsource processing within their supply chain.

Contracts are expected between controllers and processors must be compliant with Articles 28 and 29 of the GDPR and the ICO has provided further draft guidance[10] on the topic. Contracts compliant with the GDPR requirements are expected to be in place by the end of the implementation period on 25th May 2018.

Whilst provision is made for certifications and template clauses to be used to provide assurance, no such items exist at the time of this document's publication.

Fines are not the only risk you face (don't believe the hype)

It is often argued that the reason for conforming with the governance requirements of the GDPR are the large fine regimes that can be applied. However, the ICO has made it clear that the multi-million figures being mooted in the press are not likely to transpire[11].

Evidence of this approach is provided in the recent Deepmind Review[12], which concluded that there was a lack of compliance with not only the existing Data Protection Act, but also the requirements of Tort law (the foundations of English and Welsh law). The opinion that the underpinning fabric of law had been breached would lead you to assume that this was serious, and you would expect that the ICO would have taken strong action; yet nothing more happened than a commitment and formal undertaking.

However, this is not to say that there will be no financial penalty from failing to comply with basic requirements for information governance. Oxford University endured over £116,000 in costs merely from complying with a subject access request from one of its employees[13].

The impact from class actions could also be significant, as shown by the recent judgement on the class action by staff against Morrisons[14]. Showing that the controller is liable for the actions of a staff member is going to be the subject of an appeal, but it shows that a controller can be held accountable for the failures in the wider legal framework outside of the data protection requirements, and that claims for damages can be raised.

"Accordingly, thus far, I cannot conclude that the DPA excludes common law and equitable actions in respect of the same data disclosure." – Langstaff J

---

[10] https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf
[11] https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/
[12] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/
[13] http://www.hendersonchambers.co.uk/wp-content/uploads/2017/03/Data-Protection-Alerter-on-Deer-v-University-of-Oxford.pdf
[14] http://www.5rb.com/case/various-claimants-v-wm-morrison-supermarket-plc/

With Subject Access Requests (SARs) becoming free after the implementation period in May 2018, costs of servicing these requests could also rise if the general public increase the amount of requests they make.

Again, whilst there has also been an inordinate amount of attention on the requirements of complying with the 72-hours notification requirement for breaches, the impact could well increase in the light of the Article 29 Working Party guidance on the subject as previously discussed which goes beyond Cyber breaches and into information governance.

Grasping the business opportunity from complying with the GDPR

Through better understanding of information resulting from complying with GDPR, we can address a very real issue that is occurring – a recent parliamentary report at the end of 2015[15] estimated that over 90% of information circulating the internet had been created in the past two years.

Combined with recent estimates[16] that 54% of data is unknown in terms of its contents (also called dark data), where resources are being wasted in protection and storage, we can not only embrace Cloud computing but also address the amount of unknown information held within our datasets through effective risk management.

Addressing this challenge through better information governance will not only result in compliance, but also reduce costs and deliver opportunities.

Is all of this really new?

You may well think from the commentary surrounding the GDPR that some of these areas have been recently introduced, yet this couldn't be further from the truth.

Scoping and consent regarding processing of personal data have been applied within the current Data Protection Act 1998 and Privacy of Electronic Communications Regulation 2003 respectively, and are further reinforced through case law (e.g. scoping being defined to include B2B personal data in Durant vs FSA and Deer vs Oxford University).

There are very few truly new areas, and even some of those (e.g. requirements to provide evidence of conformance within processing activities) are already required within the wider requirements of legislation such as the Companies Act 2006.

This also means that waiting for further definition on areas that are already defined through case law before proceeding with compliance to the requirements of the GDPR (which is the third version of data protection requirements since 1984) is unwise.

[15] https://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/468/468.pdf
[16] http://www.computerweekly.com/news/4500256309/Lack-of-data-classification-very-costly-to-firms-says-survey?utm_medium=EM&asrc=EM_EDA_49210577&utm_campaign=20151029_BT%20revenue%20up%202%25%20on%20broadband%20and%20BT%20Sport%20Europe_&utm_source=EDA

Getting the right guidance

Hopefully, you will have not been surprised by any of the topics in this article. If you are, you will hopefully not have spent money on the consultants claiming that they are either certified GDPR professionals or providing a service that can make you compliant.

The reason I make this point is that there are no courses that are approved by the ICO (or any other organisation for that matter) at the time of publication. The ICO is responsible within the UK for the accreditation of certification bodies within the UK (as detailed within Article 43). There are many experienced people, but do not rely solely on their certification.

In order to get the right guidance, you need to:

- Read the GDPR
- Monitor the Article 29 Working Party guidance
- Subscribe to the ICO blogs

The ICO provide a range of guidance on their website[17], but this should be read in the context that the ICO have stated that they are waiting on the Article 29 Working Party to finalise their guidance prior to producing their own.

The ICO guidance has been circulated to the Cabinet Office SME panel, and contains a list of 12 steps to take now[18] and a self-assessment checklist[19] and the helpline for SMEs[20].

Summary

This is one of a number of revisions to the requirements that may well affect public sector suppliers, others being the Data Protection Bill[21], ePrivacy Regulation[22], and the Network and Information Systems Directive[23].

All of these are subject to consultation and implementation so there is little point in discussing these at length, although with the NIS Directive having the potential to incur a fine of £17m or up to 4% of global turnover (whichever is higher) for failings in the cyber security and resilience of essential services and the Data Protection Bill having the potential to alter the compliance requirements and derogations for certain aspects of the GDPR within the UK, these have been highlighted for awareness.

It is important to understand the wider legal context when undertaking any compliance exercise for the GDPR, as it is very likely that you will expend the same amount of effort to comply with all the 60-70 legal requirements for information handling and processing within the U.K. as you will for the GDPR. Why not try and look beyond one area and maximise return on investment?

---

[17] https://ico.org.uk/for-organisations/data-protection-reform/
[18] https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
[19] https://ico.org.uk/for-organisations/data-protection-reform/getting-ready-for-the-gdpr/
[20] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/10/new-data-protection-advice-service-aimed-at-small-organisations-preparing-for-the-general-data-protection-regulation/
[21] https://www.gov.uk/government/collections/data-protection-bill-2017
[22] https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation
[23] https://www.gov.uk/government/news/new-fines-for-essential-service-operators-with-poor-cyber-security

Current UK legislation, when viewed in the wider context, requires that UK-based public and private- sector organisations understand:

- the location of the data (how do you know where it is being stored, or if it has been deleted?)
- the format of the information (what is the asset?)
- the disclosure requirements (can you share it, and what are the requirements?)
- the retrieval requirements (the retention period and can you access the information throughout that period?)
- the handling requirements (does it need encryption, where can it be accessed from, what right of audit is there?)
- the usage requirements (what purposes was the information acquired for, how do you provide evidence that you meet those requirements?)

Even something as simple as knowing where data is being stored can be difficult to determine. There has been a lot of press recently surrounding Cloud Service Providers, who are fighting attempts from the US government to access information held within the Irish data centres.

This is to be applauded, but what if you were told that Outlook for iOS/Android may be caching your emails in the US or at least the Microsoft Cloud? This is the case at present if you are using an on-premise Exchange server at a version lower than Exchange 2010 Service Pack 3[24] or a server that isn't on a commercial version of Office 365[25].

Whilst it is important that you do prepare for the GDPR, it is advantageous to use this as an opportunity to evolve the governance culture to address the behaviours required from both the existing and forthcoming requirements.

About the author

Des Ward has been involved within information risk and governance within end user and supply organisations for over twenty years, spanning the majority of vertical sectors within the UK. Possessing a wide range of experience of assuring disruptive technologies, including Cloud and mobile platforms, over the past decade has provided him with an insight into the evolution required to address the challenges of supplying safe and reliable services to the customer.

Des has also undertaken research into how to change the value perception of security within the enterprise, which has led to him presenting at a wide range of industry events within the UK. His election to the board of Innopsis is the culmination of his work to date, and has allowed him to provide guidance on digital infrastructure to the public sector, and currently advises the Health and Social Care Network board on supplier compliance.

Twitter @securebusiness
Email des.ward@common-framework.com
des.ward@innopsis.org

[24] https://www.petri.com/outlook-ios-android-dumping-aws-q3
[25] https://blogs.office.com/2016/09/26/outlook-for-ios-and-android-is-now-fully-powered-by-the-microsoft-cloud/