The general data protection regulation: A myth-buster

Received: 5th August, 2016

Phil Lee
is a Partner in Fieldfisher's top-ranked Privacy, Security and Information Group. He holds CIPP(E) and CIPM status, and is a member of the IAPP's Privacy Faculty. Phil specialises in supporting clients to develop and manage their transatlantic (and wider) data privacy compliance programmes, having founded Fieldfisher's Silicon Valley office in the USA in 2012 — an office which he then ran for four years. He has worked on multi-jurisdictional data privacy projects covering more than 80 territories worldwide, and is particularly recognised for his expertise in international data transfer strategies (including Binding Corporate Rules), security incident response, and digital and offline marketing rules. Phil holds an MA in Computer Science from Cambridge University and a postgraduate diploma in Intellectual Property from Bristol University. He is a frequent contributor to Fieldfisher's Privacy and Information Law blog (http://privacylawblog.fieldfisher.com) and is also a contributing author to the IAPP's European Privacy: Law and Practice for Data Protection Professionals and Wolter Kluwers' Global Privacy & Security Laws. Phil trained and qualified at Denton Wilde Sapte and, prior to joining Fieldfisher, worked within the digital media team at Osborne Clarke.

Fieldfisher LLP, Riverbank House, 2 Swan Lane, London, EC4R 3TT, UK
Tel: 020 7861 4143; E-mail: Phil.Lee@fieldfisher.com

Kate Pickering
is a Senior Associate in Fieldfisher's Privacy, Security and Information Law Group and has a broad range of experience in privacy, outsourcing, telecommunications, systems integration, software development and licensing. When advising clients Kate is able to draw upon her combined degrees in information systems and law and her experience in the technology industry working with both public and private sector clients. Her extensive experience on a broad range of commercial transactions and time on secondment at two of the UK's leading telecommunications providers has given Kate valuable insight and understanding of the demands and overall commercial priorities for clients, particularly in the context of data protection issues.

Fieldfisher LLP, Riverbank House, 2 Swan Lane, London, EC4R 3TT, UK
Tel: 020 7861 4910; E-mail: kate.pickering@fieldfisher.com

Abstract The General Data Protection Regulation[1] (GDPR) is an undeniably complex piece of legislation. Privacy professionals everywhere, the present authors included, have a lot to learn and — thankfully — there have been many excellent articles written on the topic. For the most part, these focus on the changes that the GDPR will bring about and, specifically, the compliance actions that organisations must take. By contrast, less has been said about what the new law will *not* require. This might sound unsurprising (why would anyone want to know about things they do not need to do?) but it is important to remember that, during the course of its adoption, the text of the GDPR changed many times. As a result, some provisions that were originally proposed were dropped from the final law (or otherwise changed beyond recognition), and this inevitably created a certain amount of confusion. Then throw in a sprinkling of occasional misreporting, together with a chain of misinterpretations, and suddenly knowing what the law does *not* require becomes almost as important as knowing what it does require. Below, this paper sets out — in no particular order — a few of the most common misconceptions regarding the GDPR.

KEYWORDS: GDPR, data protection, regulation, compliance

CONTROLLERS DO NOT NEED DATA PROCESSING AGREEMENTS WITH PROCESSORS BECAUSE THE GDPR IMPOSES DIRECT OBLIGATIONS ON PROCESSORS

WRONG! Those of us familiar with the GDPR might not think it, but we have heard this one quite a few times. Let us set the record straight: data processing agreements are definitely still needed, and a whole host of contractual terms must now be put in place between a controller and its processor(s). Anyone suggesting otherwise would do well to consult Article 28 of the GDPR.

Article 28 sets out a number of new requirements that must be contained in contracts between controllers and processors, including subject matter and duration of the processing; nature of the processing; types of personal data being processed; obligations and rights of the controller; and confidentiality obligations for persons authorised to process personal data.

Going forward, we may also see the release of standard contractual clauses for contracts between controllers and processors (see Articles 28(7) and 28(8)).

WHEN RELYING ON CONSENT TO PROCESS PERSONAL DATA, CONSENT MUST BE EXPLICIT

WRONG! This was a hotly debated topic during the passage of the GDPR, but the final text requires that consent must be 'unambiguous' rather than 'explicit' (Article 4(11)). Explicit consent is required only for processing sensitive personal data — in this context, nothing short of 'opt in' will suffice (Article 9(2)). For non-sensitive data, however, 'unambiguous' consent will do — and this allows the possibility of implied consent if an individual's actions are sufficiently indicative of their agreement to processing.

EVERYONE NEEDS A DATA PROTECTION OFFICER

WRONG! Earlier drafts of the GDPR required organisations with over 250 employees or those processing more than 5,000 personal data records to appoint a data protection officer (DPO) — these requirements were not adopted under the GDPR.

In the final version of the GDPR, DPOs must only be appointed in the case of: (a) public authorities, (b) organisations that engage in large-scale systematic monitoring or (c) organisations that engage in large-scale processing of sensitive personal data (Article 37(1)). If you do not fall into one of these categories, then you do not have to appoint a DPO — although, in the interests of good practice, the appointment of one is still to be encouraged.

THE GDPR WILL ONLY AFFECT ORGANISATIONS IN EUROPE

WRONG! The GDPR expands the territorial scope of EU data protection law and will apply to both controllers and processors. There are three tests under which organisations could be caught by the territorial scope of the GDPR: (a) the 'establishment test' applies where processing takes place in the context of activities of an establishment of a controller or a processor in the EU, regardless of whether or not the processing takes places in the EU — see Article 3(1)); (b) the 'goods and services test', which applies to the processing of personal data of EU based data subjects by a controller or processor not established in the EU, where processing relates to the offering of goods and services, irrespective of whether a payment of the data subject is required (Article 3(2)(a)); and (c) the 'monitoring test', which applies to the processing of personal data of EU based data subjects by a controller or processor not established in the EU, where processing relates to the monitoring of their behaviour as far as their behaviour takes place within the EU (Article 3(2)(b)).

Organisations should assess whether any of their EU-based group entities process personal data (as processors or controllers), as these entities will be captured under the GDPR.

Non-EU organisations will now also be captured, and will have direct statutory obligations for their activities if they undertake processing activities (either as a controller or a processor) related to the offering of goods or services to data subjects within the EU or monitoring the behaviour of European data subjects (as far as their behaviour takes place within the EU).

CONTROLLERS AND PROCESSORS WILL ONLY HAVE TO ANSWER TO A SINGLE DATA PROTECTION AUTHORITY

WRONG! This may have been the original intent when the draft GDPR was published back in 2012, but it is not where the final law ended up. While it is true that organisations will have a 'lead' supervisory authority (Article 56(1)), other supervisory authorities can intervene if an issue relates to a controller or processor established in their member state or if data subjects in their member state are otherwise substantially affected (Article 56).

BIOMETRIC DATA ARE SENSITIVE DATA UNDER THE GDPR

WRONG(ISH)! You can be forgiven for thinking this. Biometric data can be sensitive data under the GDPR — but only if used for the purpose of 'uniquely identifying' someone (Article 9(1)). A bunch of photographs uploaded onto a cloud service would not be considered sensitive data, for example, unless used for identification purposes — think, for instance, of airport security barriers that recognise you from your passport photograph.

INDIVIDUALS HAVE AN ABSOLUTE RIGHT TO BE FORGOTTEN

WRONG! Article 17 of the GDPR refers to the 'right to be forgotten' as the 'right of erasure'. However, unlike the right to opt-out of direct marketing, it is not an absolute right. Organisations may continue to process data if the data remain necessary for the purposes for which they were originally collected (Article 17(1)(a)), and the organisation still has a legal ground for processing the data under Article 6 (and, if sensitive data are concerned, Article 9 too) — see Article 17(1)(b).

PARENTAL CONSENT IS ALWAYS REQUIRED WHEN COLLECTING PERSONAL DATA FROM CHILDREN

WRONG! Parental consent is required only if the processing itself is legitimised on the basis of consent. Article 8(1) of the GDPR sets out that in circumstances where consent is the lawful basis for processing personal data in relation to the offer of information society services directly to a child, consent is only lawful where the child is at least 16 years old. Where the child is less than 16 years, processing is only lawful if and to the extent such consent is given or authorised by the holder of parental responsibilities over the child. Member states may provide by law for a lower age — provided such lower age is not below 13 years.

However, this requirement applies only if consent is the basis for the processing. If the processing is based on another lawful processing ground (for example, compliance with a legal obligation, vital interests or possibly even legitimate interests), then parental consent is not required (Article 8(1)).

EVERY BUSINESS WILL BE SUBJECT TO NEW DATA PORTABILITY RULES

WRONG! Data portability requirements are mandated only when processing is based on consent or contractual necessity (Article 20(1)). It does not apply when, for example, processing is based on legitimate interests. This is an important strategic point for businesses to consider when deciding upon the lawful grounds on which they will process personal data.

PROFILING ACTIVITIES ALWAYS REQUIRE CONSENT

WRONG! Consent is only required if the profiling activity in question 'produces legal effects' or 'significantly affects' a data subject (Article 22(1)). The obvious implication here is for the targeted advertising industry — whether you like or loathe targeted advertising, it is a bit of a stretch to say that data processing for the purpose of serving targeted adverts has these consequences. Put another way, the GDPR does not generally mandate consent for the profiling activities of advertising technology companies.

PSEUDONYMISED DATA (EG HASHED DATA) ARE TREATED EXACTLY LIKE ANY OTHER PERSONAL DATA UNDER THE GDPR

WRONG(ISH)! The GDPR makes clear that data protection rules apply to pseudonymised data, but pseudonymised data implicitly benefit from certain relaxations under the GDPR — for example, mandatory data breach reporting may arguably not apply if data have been securely pseudonymised (Article 33 — on the basis that securely pseudonymised data are 'unlikely' to create risk). See also Article 11, which seemingly relaxes certain data subject rights for pseudonymised data.

THE GDPR WILL REDUCE PAPERWORK FOR ORGANISATIONS AS THE NOTIFICATION REQUIREMENT WILL BE SCRAPPED

WRONG! The information currently contained in notifications to data protection authorities will still have to be gathered internally for the purposes of fulfilling the record-keeping requirements under the GDPR (Article 30 and recital 56). These record-keeping requirements will apply to both controllers and processors, must be in writing (including electronic form) and shall contain, among other things: purposes of the processing; categories of data subjects and categories of personal data; transfers of personal data to third countries or international organisations; time limits for erasure; and where possible, a general description of the technical and organisational security measures in place (Article 30).

Businesses will need to ensure these records are kept up to date as each controller and processor will 'be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations' (recital 82). There is however some reprieve for small to medium-sized enterprises: the GDPR includes a derogation at Article 30(5) for organisations with fewer than 250 employees, unless the processing is risky, not occasional, or involves special categories of data or criminal data.

MY ORGANISATION IS COMPLIANT UNDER THE DIRECTIVE, SO THERE WILL NOT BE TOO MUCH WORK INVOLVED IN BECOMING GDPR COMPLIANT

WRONG! While being compliant under a member state's law which implements the Directive (for example, the Data Protection Act 1998 in the UK) is a step in the right direction, it bears repeating that the GDPR is a complex piece of legislation. Becoming GDPR compliant will differ from business to business and requires understanding how your business uses data today — for example, are you a processor or a controller, do you process 'ordinary' personal data or 'sensitive' personal data (or both)? Are you within territorial reach of the GDPR? What is your strategy for exporting data? The answers to these questions (and more) will affect your business's compliance model and the steps necessary to become GDPR compliant.

I'VE GOT TWO YEARS TO IMPLEMENT THE GDPR SO I DO NOT NEED TO WORRY ABOUT IT JUST NOW

WRONG! The GDPR entered into force in May 2016 and will be directly applicable from 25th May, 2018. In other words, that two-year implementation period is already marching on. Any business entering into long-term contracts should be considering this now. Compliance is a time-consuming process and the number of changes required will depend on the nature of the organisation. Organisations will need to prioritise the actions that present the highest risk if not taken. The time it takes for most organisations to assess, prioritise and action compliance measures should not be underestimated.

THE UK HAS VOTED TO LEAVE THE EU, SO THERE IS NO NEED TO WORRY ABOUT THE GDPR

WRONG! It will take the UK at least two years to negotiate an exit from the EU. In the interim, the UK will remain fully subject to EU laws, including the GDPR once it comes into effect. Notwithstanding what model the UK chooses to follow with regard to its exit from the EU, the GDPR will apply to every business — whether in the EU or not — that offers goods and services to the EU. Therefore, many UK businesses will still be subject to GDPR requirements, as will wider international businesses operating across the UK and the EU.

A spokesperson from the UK's data protection authority, the Information Commission's Office, stated in response to 'Brexit' that the UK will still be required to provide 'adequacy' if it wants to trade with the Single Market.[2] This means that the UK's data protection standards will have to be equivalent to the EU's General Data Protection framework starting in 2018.

Despite the uncertainty regarding how the UK will exit from the UK, it is clear that businesses should continue to undertake their GDPR readiness preparation and the UK's leaving the EU should not change this.

A FINAL WORD

That is it for our top 15 list. So, consider yourself informed — and next time you hear any of these come up in conversation, be sure to show off your data protection prowess and set the record straight!

References

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th 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).
2. Wood, S. (2016) 'GDPR still relevant for the UK', available at: https://iconewsblog.wordpress.com/2016/07/07/gdpr-still-relevant-for-the-uk/ (accessed 15th August, 2016).