Cybersecurity, Data Privacy & Information Management
Alert

Weil

June 6, 2018

Top Five GDPR Myths – Busted!

By Barry Fishley and Briony E Pollard

With the GDPR now in force, we consider the top five GDPR myths and set the record straight.

1. MYTH: You MUST have consent to process personal data

TRUTH: No doubt you will have received (and probably still receiving!) emails from organisations stating that under the General Data Protection Regulation ("**GDPR**") they require your consent to continue to contact you after 25 May 2018. Such emails are often unnecessary and, in some cases, unlawful. At best, they confuse two distinct points: (1) holding personal data, which is governed by the GDPR; and (2) direct marketing by email and/or SMS using personal data, which is governed by the Privacy and Electronic Communications Regulations (the "**PEC Regs**").

Processing (which includes holding) of personal data is lawful under the GDPR provided at least one of the processing conditions in Article 6 applies. Obtaining consent from the data subject is only one of these processing conditions. Accordingly, seeking consent to process personal data may be unnecessary if another processing condition exists. An organisation may lawfully process a data subject's personal data if it is, for example, necessary for the performance of a contract. Even if an organisation relies on consent, that does not mean they need renewed consent. Recital 171 states that organisations can rely on existing consent provided it is in line with GDPR requirements, i.e. freely given, specific, informed and unambiguous. In any event, relying on consent as a processing condition is a risk as it can always be revoked.

The PEC Regs govern marketing to individuals by electronic means (including emails and texts). Organisations must obtain consent from an individual to market to them in this way or rely on the so-called 'soft opt-in' (i.e. where the individual is an existing customer and the communication concerns similar products/services) provided that the individual is given information on how they may 'opt-out' of communications in every communication sent to them.

Accordingly, seeking to renew consent comes with pitfalls. If the organisation receives no response, it will not be able to market to those data subjects, as they will not have consent for it to do so.

Some organisations have used the introduction of the GDPR as an opportunity to cleanse their databases, but in doing so run the risk of decimating their database of data subjects to whom they may market.

Further, emailing an individual, who is not a previous customer, asking for consent to market to them is considered a marketing communication and is therefore unlawful if the organisation does not have their consent (which meets GDPR requirements) to do so.

2. MYTH: Regulators such as the UK Information Commissioner's Office (the "ICO") will impose huge fines on organisations, and will make early examples of organisations

TRUTH: Under the GDPR, the ICO has the power to issue maximum fines for serious breaches of EURO 20million or 4% of worldwide turnover (whichever is the higher). However, the ICO said, "*it is scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm*" and that "*hefty fines will be reserved for those organisations that persistently, deliberately or negligently flout the law*". The ICO never invoked their maximum powers under the Data Protection Act 1998 (i.e. fines of up to £500,000) and has stated that it intends to use its powers under the GDPR "*proportionately and judiciously*".

When determining the severity of pecuniary sanctions, the ICO will take into account the organisation's cooperation with the ICO following breaches. It is also worth remembering that a fine is only one of the measures included in the GDPR to encourage compliance.

3. MYTH: All personal data breaches need to be reported to a supervisory authority, such as the UK's ICO, and as soon as the breach occurs

TRUTH: Not true. The threshold to determine whether an incident needs to be reported to the supervisory authority depends on the risk it poses to the individual whose data has been compromised. Reporting of a personal data breach to the ICO is mandatory under the GDPR only if it is likely to result in a risk to the rights and freedoms of natural persons. A notification must be made without undue delay, and where feasible, not later than 72 hours after having become aware of it.

If there is a likelihood of a high risk to natural person's rights and freedoms, organisations need to report the breach to the individuals whose personal data has been affected without undue delay. ICO guidance indicates that high-risk situations are likely to include the potential of individuals suffering significant detrimental effect. The risk of identity theft seems a likely example of this.

4. MYTH: GDPR creates an EU-wide harmonised set of rules. If an organisation is compliant in one EU country it is compliant in all

TRUTH: The creation of a set of rules, harmonised across the EU, was a desired outcome of the GDPR. However, whilst there is more consistency across the EU, the numerous derogations granted to Member States mean that there are no fully harmonised rules. Furthermore, some Member States will continue to have their own local laws which will continue in effect irrespective of the GDPR. In addition, each independent supervisory authority will issue its own guidelines and decisions, so there may be differences of approach. This all means that organisations will need to understand and/or seek local advice on each country's specific rules and have flexibility in their technology and processes to ensure compliance across all EU countries where it operates.

5. MYTH: Every organisation needs a Data Protection Officer ("DPO")

TRUTH: An organisation must designate a DPO where (i) the processing of personal data is carried out by a public authority or body (except for courts acting in their judicial capacity); (ii) the core activities of the controller or processor consist of processing operations which, by virtue of their nature, scope and/or purpose, require regular and systematic monitoring of data subjects on a large scale; or (iii) the core activities of the controller or processor consist of processing on a large scale of special category data and personal data relating to criminal convictions and offences.

When determining if processing is on a "large scale", ICO guidelines state that the number of data subjects concerned; the volume of personal data processed; the range of different data items

processed; the geographical extent of activity; and the duration of the processing activity should be considered. Typical examples of organisations, which process personal data on a “large scale”, include hospitals, insurance companies and certain telecommunications service providers.

It is also worth noting that local laws in Member States (such as Germany) may separately set out requirements for a DPO, apart from the requirements of the GDPR.

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any member of the Cybersecurity, Data Privacy & Information Management Group.

Barry Fishley	View Bio	barry.fishley@weil.com	+44 20 7903 1410
Briony E Pollard	View Bio	briony.pollard@weil.com	+44 20 7903 1372