ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Top 10 — Europe’s Proposed General Data Protection Regulation

Technology, Privacy, and eCommerce

This year, it has been increasingly important for in-house counsel to keep tabs on the progress of EU data protection and privacy reform. Europe's Data Protection Directive (95/46/EC) (the Directive) is now more than 20 years old and, for some time now, the EU's legislative bodies have been working on a replacement. The overall intent is to update, but also to introduce greater harmonisation of these rules across EU members states. In early June 2015, we learned that the Council of the EU has reached a "general approach" on Europe's proposed General Data Protection Regulation (the Regulation), with the twin aims of enhancing Europeans' data protection rights and increasing business opportunities in the Digital Single Market.

The Regulation remains subject to some significant negotiation and is unlikely to come into force until 2017–2018. If you represent any business touching upon personal data you should start considering the future rules and what they mean for your business, not least as there are potentially some significant changes. Importantly, the new rules will be implemented by a legal act known as a "Regulation" which, under EU rules, would be "directly applicable" in all EU members states. Effectively this means the members states do not have to implement the rules into their national laws, and they cannot delay or vary the rules coming into effect. The objective is a far more consistent set of rules applying to personal data across the Europen Union.

Like many organizations, the Fieldfisher privacy and information team is monitoring the progress of the legislative changes, and we are cautious of recommending any significant preparatory steps until the exact make-up of the final rules are better understood (hopefully in early 2016).

If the new law does get passed early in 2016 — what are the top 10 issues you should be aware of?

1. **Out-of-scope today, in scope in the future — what's caught?** You may be subject to the

new regime even if you are not required to comply with the current one. Even if you are not established in the European Union, you may be caught by the new rules if you are a data controller whose processing activities are directed at EU residents, and/or you process personal data in relation to offering goods or services to, or monitoring the behaviour of, EU residents. One of the more significant changes is that data processors established in the EU will fall within aspects of the proposed Regulation (with new obligations on processors specifically outlined).

2. **You may be processing more personal information than you think.** The definition of "personal data" proposed under the new regime is very broad. Unique identifiers (e.g., IP addresses) that can single individuals out are likely to be included expressly within the definition. It is possible that pseudonymous data (e.g., information that can single individuals out, but does not directly identify them) would be subject to lower data protection standards. However, such data would become personal data if profiling activities enable the identification of individuals from the data. The updated concept of "sensitive data" is likely to include genetic data.
3. **If you receive personal data from a third party, you may need to "re-think" your legal justification for processing it.** Under the current regime, the "legitimate interests" pursued by a business or a third party to whom the business discloses personal data is a valid lawful justification for processing personal data. The ability of third parties, to whom personal data are disclosed to rely on this lawful ground for processing, is under threat under the proposed new regime. In addition, "consent" as a lawful ground for processing is likely to be subject to very tight and strict conditions. It may be necessary to revisit the prior basis of consent for certain data, and this is an area where businesses may be able to vary existing data collection practices in order to preempt changes to consent mechanisms, which provide more flexibility in the future.
4. **You are likely to need to take account of individuals' new and enhanced rights.** There are a number of proposed tweaks to existing rights, for example, a requirement to provide additional information in response to a subject access request and a prescribed way of presenting the right to object to direct marketing. New data subject rights are also proposed, for example, "the right to be forgotten" and a new right of "data portability." This latter right may mean that businesses will be required to provide copies of personal data records in a standardised electronic data format. This is an area subject to heavy lobbying and is likely to be further negotiated over the months to come.
5. **Your big data analytics and profiling activities may be seriously curtailed.** Under the proposed new regime, explicit consent is likely to be required in most instances in order to process personal data for profiling. Businesses should identify the nature of any profiling activities that they undertake and think creatively about possible consent mechanisms.
6. **Think privacy — you will need to design your products and services for compliance and minimise the personal data processed.** Under the proposed "privacy by design" requirement, you will need to design compliant policies, procedures and systems at the outset of product development and keep them under review. One of the key aspects of the proposed "privacy by default" principle is that, by default, only personal data that are necessary for a specific purpose are to be processed. This principle is likely to have a significant impact on some businesses' processing operations if the implications are that cookies that process personal data will need to be switched off by default.
7. **Accountability principles need to be reviewed.** The draft proposal introduces an accountability principle which imposes significant documentation requirements. Businesses should review their existing data protection policies and procedures to ensure that they meet the expected standards.
8. **Another form of accountability is the perhaps inevitable emergence of breach**

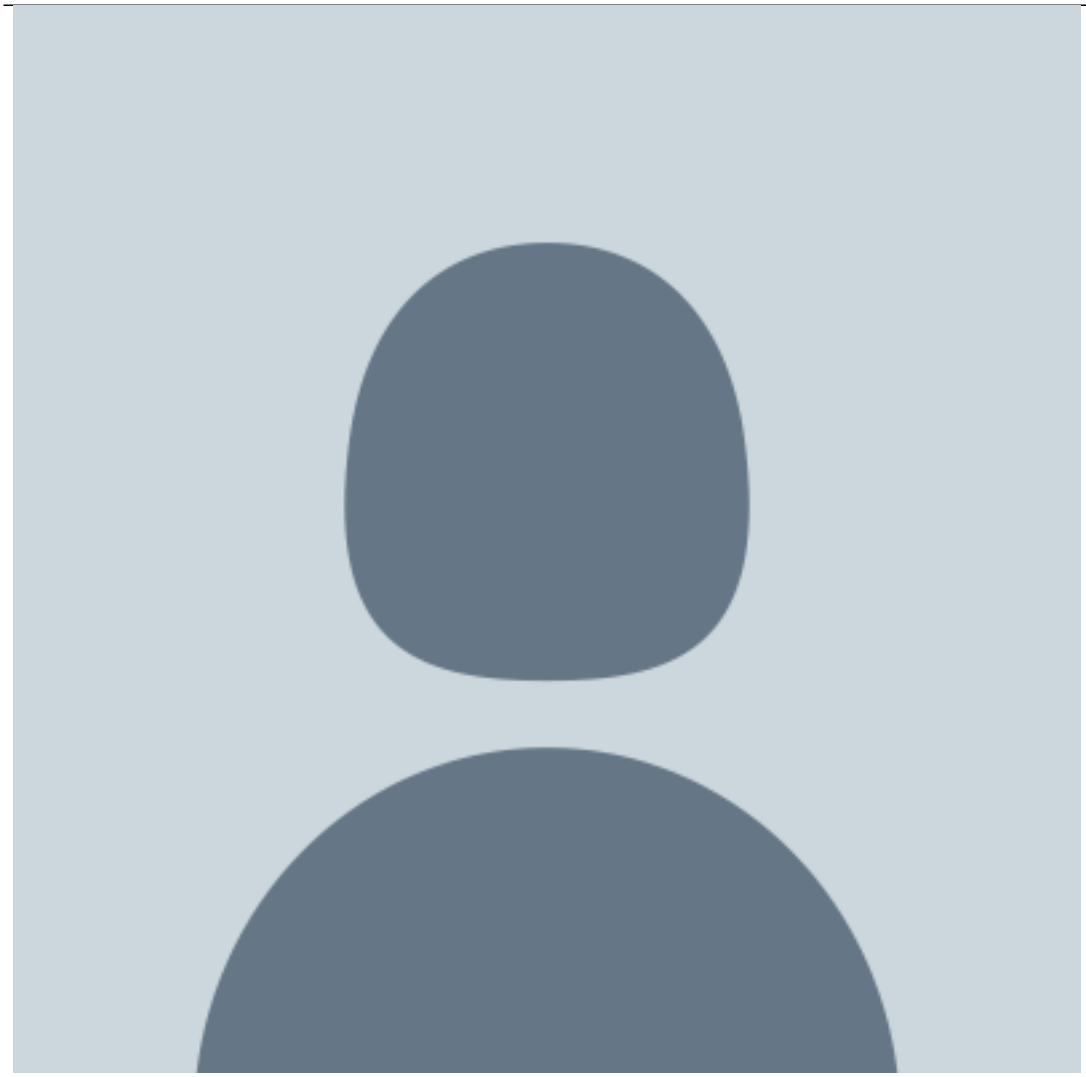
notification rules. Although some Member States have phased in their own rules in recent years, away from telecoms industry specific rules, Europe has not yet imposed data breach notification obligations on EU based data controllers. This heralds another change, the Regulation will almost certainly impose a more proactive approach to data security and introduce a general obligation to report data breaches to affected data subjects “without undue delay” (but after the breach has been reported to the applicable supervisory authority).

9. **You may need to appoint a data protection officer.** Under the EU Commission’s proposal, a data controller or processor must designate a data protection officer (DPO) for a minimum initial period of two years in certain specified circumstances, if it regularly and systematically monitors individuals. Any business that carries out profiling activities is likely to be regarded as engaging in processing operations, which satisfy this description.
10. **Data transfer restrictions are here to stay.** You will still have to jump through hoops in order to legitimately transfer data outside of Europe. It may well transpire that “Binding Corporate Rules” (BCRs) gain even more compliance prominence. The Commission’s proposal expressly acknowledges the validity of BCRs, including BCRs for processors, as a valid legal solution to EU’s strict data export rules. To date, BCRs have had only regulatory recognition, and then not consistently across all member states, casting a slight shadow over their longer term-future. Express legislative recognition ensures the future of BCRs — they’re here to stay.
11. **Enforcement to have more teeth and noncompliance greater consequences.** There are likely to be serious financial repercussions for non-compliance — now is a good time to get data protection priorities right! The Commission’s proposal includes very harsh fines for breaches of data protection law — as high as two percent of the global revenue of a commercial enterprise (other drafts suggest the greater of €100m or five percent annual worldwide revenue). Where you are established as a data controller in more than one member state, it is the data protection authority of your country of main establishment that will be competent to decide — this is known as the “one stop shop” principle.

Conclusions

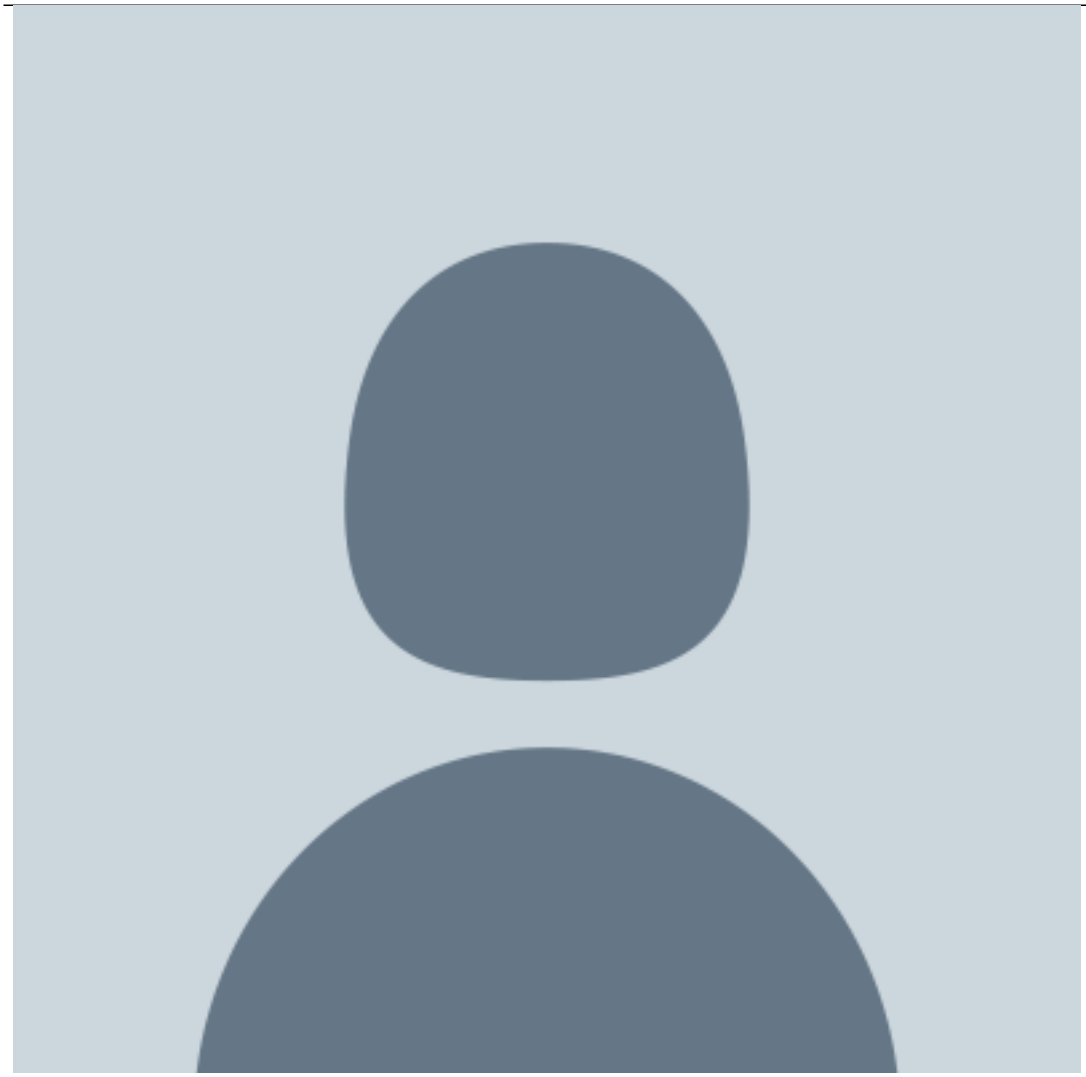
There is a lot to think about and the devil is in the details. Your main take away is that Europe doesn’t have a new data protection law yet. In fact, far from it — we’re still only at the draft stage! And until we have agreed the final text of the new law, it’s very difficult to predict where exactly we will land on many of the issues. This said we do appear to be in the home straight. Deciding how to get ready for the Regulation at this stage is difficult — what’s clear is that understanding and complying with today’s Directive (as implemented) and its principles is probably one of the best preparedness steps you can take.

Mark Webber



Field Fisher

Leonie Power



Field Fisher