Briefing

Data Protection

BURGES SALMON

February 2016

# Seeing the wood for the trees: Which aspects of the new General Data Protection Regulation should you focus on?

The EU's governing bodies recently reached an agreement on the text of the new General Data Protection Regulation ("GDPR") after months of ongoing trilogue negotiations.

The GDPR, which will replace the existing EU directive, must now be formally approved by the EU institutions. This is expected to occur in spring 2016, with its provisions taking effect two years later.

The new requirements will apply to public authorities and private entities, both within and outside the EU, that control and process the personal data of EU residents. As the GDPR is over 200 pages in length, this guide provides a summary of its key provisions, the impact it may have and what you can do now to prepare for its implementation.

| Topic | Position under the GDPR | Implications |
|---|---|---|
| **Scope of GDPR** | | |
| **Extra-territorial reach** | The GDPR will apply whenever EU residents' personal data is processed in connection with: (1) the offer of goods or services; or (2) monitoring of behaviour within the EU (such as the analysis of consumers' preferences). This will be the case even if the organisation processing the personal data has no physical presence in the EU. | Where an organisation outside the EU has to comply with the GDPR, it must appoint a representative within one of the Member States in which it supplies goods or services or monitors the behaviour of EU citizens. |
| **What data is covered?** | The GDPR applies to the processing of 'personal data', which broadly retains its current meaning as any information relating to an individual. However, the scope of the definition is broadened to include online identifiers (such as cookies).<br>The existing concept of 'sensitive personal data' has also been broadened, to include genetic and biometric data. | Organisations should review what data they process for the purpose of assessing whether an individual is 'identifiable' from such data and, therefore, whether the GDPR applies. |
| **Obligations on data processors** | Data controllers remain liable for the acts of processors, however, in some areas responsibilities are also placed on data processors directly; for example, processors must obtain prior consent to sub-processing and data transfers outside the EEA, as well as complying with notification obligations concerning data breaches. | Contracts for the appointment of a processor must be reviewed to ensure compliance with the provisions of the GDPR. It is likely that pro forma contracts will be issued in due course. |
| **Imposition of further obligations** | | |
| **Lawfulness of processing** | 'Consent' remains one of the grounds for the lawful processing of subjects' data. However, this requires a higher threshold than before – consent must be 'freely given, specific, informed and unambiguous'. This is higher still for sensitive personal data, which requires that an individual's consent is 'explicit'. | Given the higher threshold of 'consent' adopted, organisations should put in place clear and affirmative agreements if they wish to rely on this justification. Silence, pre-ticked boxes or inactivity will no longer suffice. Retaining records to evidence subjects' consent is also important - companies bear the burden of proof. |
| **Transparency requirements** | The GDPR extends the information that an organisation must provide to individuals concerning the processing of their data. | Organisations will need to review their privacy notices and policies to ensure that the necessary information is provided to individuals. |

*continued over*

| | | |
|---|---|---|
| **Accountability provisions** | The GDPR imposes further accountability measures, including appointing a Data Protection Officer (DPO) where processing: (i) requires regular and systematic monitoring of data subjects; (ii) involves sensitive personal data on a large scale; or (iii) is carried out by a public authority. | Clear policies should be put in place to ensure that the GDPR's accountability provisions are followed. In addition, a culture of compliance should be embedded, aided by staff training where necessary. |
| **Notification of privacy breaches** | Each member state must appoint a Supervisory Authority (SA) for compliance purposes.<br>Where a personal data breach has occurred, data controllers must notify the SA within 72 hours (unless the breach is unlikely to pose a risk to individuals' rights). | Internal policies should be revised to ensure that data breaches are dealt with in the right way. |
| **Transfer of data overseas** | The current system is maintained, in so far as the transfer of personal data outside the EEA is permitted: (i) by way of an EU-wide 'adequacy decision'; (ii) pursuant to model contractual clauses or binding corporate rules; or (iii) under certain limited derogations. | Very little has changed regarding data transfers outside the EEA, although the adequacy of countries' data protection laws will now be measured against the higher standards imposed by the GDPR. |
| **Rights afforded to data subjects** | | |
| **Right to be forgotten** | An individual will be able to require the erasure of their personal data in certain situations, and to require the data controller to inform others to do the same (eg to delete links to that data). | The duty to inform other controllers of a subject's request for erasure appears burdensome. However, this is limited to what steps are 'reasonable' given the technology and costs involved. |
| **Data portability** | Where data is processed based on an individual's consent, he can require the existing controller to 'port' the data – in a useable format – to a new controller. | Although the right to data portability is qualified to take account of technical feasibility, organisations should ensure that they have the resources to deal with such requests. |
| **Governance and enforcement provisions** | | |
| **'One stop shop'** | Currently, organisations are subject to enforcement action by the data protection authority in each Member State in which it operates.<br>In contrast, under the GDPR, multi-national organisations will have one lead SA: the SA located in the Member State in which it has its main establishment. | Further guidance is anticipated regarding the meaning of 'main establishment' and therefore the identification of lead SAs. This may include disincentives against 'forum shopping'. |
| **Sanctions for non-compliance** | Enforcement powers will be significantly increased under the GDPR, including the fines that may be levied. For the most serious infringements, fines up to 4% of a company's annual worldwide turnover may be imposed. | Given the substantial fines that can be imposed, organisations should invest time and resources into ensuring compliance with the GDPR. |
| **European Data Protection Board** | A new European Data Protection Board (EDPB) will be established, in replacement of the Article 29 Working Party (A29WP).<br>The EDPB will be formed of representatives from the various SAs and a representative from the European Commission. It will have an advisory function (as with the A29WP), but it will also have enforcement powers. | |

## Contact:


**Andrew Dunlop**
Partner

+44 (0)117 902 2786
andrew.dunlop@burges-salmon.com

**Annabelle Gold-Caution**
Solicitor

+44 (0)117 902 7202
annabelle.gold-caution@burges-salmon.com