# SAVE THE DATA: EU GENERAL DATA PROTECTION REGULATION TO APPLY FROM 25 MAY 2018

06 May 2016 | London
Legal Briefings – By **Miriam Everett**

The EU General Data Protection Regulation has finally been approved and published in the Official Journal. The countdown to its application date of 25 May 2018 has therefore begun.

The European Commission published its first draft of the EU General Data Protection Regulation (the "**GDPR**") in January 2012, a comprehensive reform of current the existing EU regime. In April 2016, after over four years of debate, the final text of the GDPR was formally approved.

The GDPR has now been published in the Official Journal (on 4 May 2016) and will enter into force on the 20th day following that publication (i.e. on 25 May 2016). There is then a two year implementation period, meaning that it will apply from 25 May 2018.

This eBulletin gives an overview of some of the key compliance issues for organisations in relation to the GDPR, including as to data security and sanctions which are not only relevant from a pure data protection compliance perspective, but also in the broader context of data issues and cyber security.

## BUSINESS IMPACT SUMMARY

- Extra-territoriality – the GDPR will extend to data controllers located outside of the EU who offer goods and services to EU citizens or monitor their behaviour.
- Fair Processing Information – the GDPR will require data controllers to provide more information to data subjects in their fair processing notices.
- Consent – consent will need to be freely given, specific, informed and unambiguous,

involving a clear affirmative action on behalf of the data subject.

- Rights of the Data Subjects – the GDPR will provide more transparency for data subjects with respect to the processing of their data, as well as enhanced rights to rectify, delete, restrict, or object to, data being processed. There will be additional obligations on data controllers when dealing with subject access requests, save that manifestly unfounded or excessive requests may be refused.

- Controller/Processor Accountability – the GDPR will give statutory recognition to best practice concepts such as data protection by design, imposing greater accountability on data controllers, as well as placing data processors on the hook for certain regulatory liability for the first time.

- International Transfers – binding corporate rules will be given statutory recognition; criteria for adequacy decisions are set-out, and new possibilities for adequate protection are provided in the form of codes of conduct and certifications.

- Data Protection Officer – the appointment of a data protection officer will be mandatory for organisations processing sensitive personal data on a large scale or monitoring data subjects.

- Security – the GDPR will set-out slightly more detailed requirements for security of data but the responsibility for determining appropriate security measures will remain with the data controller.

- Data Breaches – the GDPR will introduce a new mandatory requirement for data controllers to notify the regulatory authority of personal data breaches within 72 hours.

- Sanctions – the GDPR will provide for two tiers of sanctions, with maximum fines of up to EUR 20 million or 4% of annual worldwide turnover, whichever is greater.

- Guidance, Codes of Conduct and Certifications – the GDPR sets out certain areas where we can expect/hope to either see further guidance in the future from the new European Data Protection Board, or potentially the development of approved Codes of Conduct and/or certification mechanisms.

## EXTRA-TERRITORIALITY

According to Article 3 of the GDPR, it will not only apply to organisations established within the European Union, but also to organisations located outside of the European Union but offering goods or services to, or monitoring the behaviour of, European data subjects.

The Recitals give some guidance regarding the interpretation of "monitoring" in Article 3, providing that monitoring would include the tracking of individuals on the internet to profile them for the purposes of analysing them or predicting their personal preferences.

The GDPR therefore extends the scope of current data protection regulation. Technology companies in particular, who may currently locate their servers outside of the EU and therefore be out of scope of the existing data protection regime, may now find themselves subject to the GDPR if they are targeting EU customers. Questions remain regarding the effective enforceability of these new data protection obligations against non-EU controllers, but there is no doubt that the long arm of EU data protection law is seeking to reach beyond EU borders.

The GDPR allows Member States during the two year period for implementation to deviate from the Regulation to make more specific rules to ensure the protection of the rights/freedoms in respect of processing employee personal data in the employment context. This expressly includes measures for, among other things, the transfer of data between group companies and monitoring in the workplace. Employers will need to be alert to these further amendments.

## FAIR PROCESSING INFORMATION

Articles 13 and 14 of the GDPR set out details of the so-called fair processing information to be provided to individuals about the processing of their personal data.

The requirements are much more detailed than those under the current Data Protection Act 1998, which requires that fair processing notices should simply include details of: (i) the data controller's identity; (ii) the purpose or purposes for which the data controller intends to process the information; and (iii) any extra information the data controller needs to give individuals in the circumstances to enable it to process the information fairly. The GDPR provides that data controllers should provide the data subject with significantly more information, including:

- details of the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;
- where the processing is based on the data controller's legitimate interests, details of those legitimate interests;
- where the processing is based on consent, the existence of the data subject's right to withdraw consent at any time;
- the existence of the data subject's rights, including the right to make subject access requests, the right to rectification and deletion of personal data, and the right to make a complaint to the regulatory authority; and
- where the data controller intends to transfer the personal data to a third country, details of such transfers, including the appropriate safeguards in place.

Whilst this is a more detailed legal requirement for data controllers than under the current regime, it is fair to say that the additional information required to be given to data subjects is broadly in line with current market best practice advice (at least in the UK). What the GDPR appears to be seeking to do, is making current voluntary best practice now a mandatory legal requirement, with a few added bells and whistles. Organisations will therefore need to undertake a comprehensive review of their current practices in order to be able to carry out a gap analysis and identify what changes (if any) need to be made in order to bring them into line with the new requirements.

## CONSENT

Consent is defined in Article 4 of the GDPR as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed.

The requirements for "unambiguous" consent and for a "clear affirmative" action on the part of the data subject are both new, and likely to have significant implications for data controllers with respect to how they go about gathering data subject consent. In particular, the requirement for clear affirmative action means that silence, pre-ticked boxes or inactivity will no longer constitute valid consent.

The GDPR does not invalidate consent given by employees in the employee/employer context. However, the Recitals state that, in order to safeguard that consent has been freely-given, it will not be a valid legal ground for data processing where there is a clear imbalance between the data subject and the controller. It therefore seems likely that consent will be interpreted very narrowly in the context of employee consent, leaving employers to consider other ways in which they can justify the processing of employee data.

It is worth noting that, despite considerable debate around the subject, there remains a distinction in the GDPR between the type of consent required for processing of personal data and that required for the processing of sensitive personal data. Processing of sensitive personal data will require the "explicit" consent of the data subject.

## RIGHTS OF THE DATA SUBJECTS

There are various themes running through the GDPR. One such theme relates to the rights of data subjects and transparency with respect to the processing of personal data. The GDPR places numerous obligations of transparency on to data controllers. Under Chapter III of the GDPR, data controllers are required to provide a significant amount of information to data subjects, both at the time of collection of the data (see the paragraph relating to "Fair Processing Information" above) and also in the event that the data subject makes a subject access request, including the purposes and detail behind the processing (e.g. what legitimate interests were being pursued, details of transfers outside the UK and suitable safeguards to protect the personal data, as well as how long the information is being held). Whilst the concept of subject access rights is not new, the obligation on data controllers to provide additional information to the data subject (e.g. informing the data subject of his/her right to request rectification or erasure of data or to object to the processing of their personal data, the right to withdraw their consent, and to lodge a complaint with the regulatory authority) increase the already significant administrative burden associated with responding to such requests.

Furthermore, Article 12 of the GDPR provides that information provided in response to a subject access request must be provided by the data controller free of charge unless the request is manifestly unfounded or excessive in which case a reasonable fee may be charged (with no guidance as to how either should be interpreted). The GDPR also gives the data controller the option to refuse to act on a request where it is manifestly unfounded or excessive, but the data controller has the burden of showing this. Data controllers also only have one month in which to respond to a subject access request, although this time period can be extended by up to two months where necessary, taking into account the complexity of the request and the number of requests.

Overall, although the process for dealing with subject access requests does not appear to be hugely different under the GDPR to that with which organisations are already used to dealing, it remains to be seen whether the enhanced transparency obligations will further encourage data subjects to make more of these types of requests in the future.

In addition to the right of subject access, data subjects will have other express rights under the GDPR: the right to rectification (i.e. rectifying inaccurate personal data); the right to be forgotten (i.e. the right to deletion of personal data in a number of situations); the right to restrict, or object to, processing of their personal data and the right to data portability (i.e. to receive their personal data in a structured, machine-readable format).

## CONTROLLER/PROCESSOR ACCOUNTABILITY

There is also a general theme of data controller accountability running through the GDPR. Enhanced levels of transparency for data subjects (see paragraphs on "Fair Processing Information" and "Rights of Data Subjects" above for further details) mean that data controllers will be made to be held more accountable for their data processing actions than under the current Directive.

In addition, Article 25 of the GDPR gives statutory recognition to the concept of "data protection by design". This concept is not a new one and has been promoted by regulators (at least in the UK) as a best practice method of data protection compliance for some time. However, the GDPR is once again turning such best practice into a statutory requirement.

The GDPR also sets out more detailed legal requirements to apply to the controller/processor relationship, and to processors in general. Article 28 of the GDPR sets out a number of requirements for the contract between data controllers and data processors and also provides that these requirements may be set out in some form of standard contractual clauses under Member State law. This may therefore be an area where we can expect to see further guidance in the future and potentially the introduction of controller/processor standard clauses similar to the ones already available for international transfers.

The GDPR also makes data processors directly subject to regulation for the first time. Article 29 of the GDPR directly prohibits data processors from processing personal data except on instructions from the data controller. Breach of this provision could result in an administrative fine of up to EUR 10 million or 2% of annual worldwide turnover whichever is greater. Article 32 of the GDPR also extends data security obligations to data processors as well as data controllers (see paragraph on "Security" below for further details).

## INTERNATIONAL TRANSFERS

Although many aspects of the GDPR have been criticised for being overly bureaucratic, the international transfer provisions appear to provide a little more scope for organisations to transfer data overseas in a compliant manner.

In particular, the GDPR provides that adequacy decisions made by the European Commission can apply to specific processing sectors or territories within a country, as well as to a country as a whole. This could result in future adequacy decisions finding specific industry sectors or states to provide adequate protection for data. For example in the USA, where sector specific or state specific privacy legislation may provide adequate protection despite there being no overall data protection law at a federal level. The GDPR also clarifies the process by which adequacy decisions should be made, setting out detailed criteria on which the European Commission should consult.

In addition, the GDPR removes any uncertainty relating to the effective scope of binding corporate rules ("**BCRs**"). The GDPR provides statutory recognition for BCRs, as well as a clearly defined process for their approval, as set out in Article 47. According to Article 47, provided that any submitted BCRs are legally binding, confer enforceable rights on data subjects and satisfy certain further requirements as to their content, then they should be approved by the appropriate regulatory authority.

The GDPR also introduces two new grounds for adequate international data transfers, being transfers subject to an "approved code of conduct" or an "approved certification mechanism" (see paragraph on "Guidance, Codes of Conduct and Certifications" below for further details).

The whole issue of international transfers remains the subject of much debate at the moment, with the European Commission considering approval of the new proposed EU-US Privacy Shield following the invalidation of the US Safe Harbor by the Court of Justice of the European Union in October last year. For further details regarding transatlantic data transfers and the proposed Privacy Shield, please see our bulletin, available here.

## DATA PROTECTION OFFICER

Previous drafts of the GDPR suggested that data controllers would be subject to a new mandatory requirement to appoint a specially trained data protection officer ("**DPO**") with a long list of qualifications, to take responsibility for the organisation's compliance with the GDPR. This requirement would apply to any organisation employing more than 250 people or processing personal data relating to 5,000 or more data subjects.

The final position appears to be clear cut. Section 4 of Chapter IV of the GDPR provides that the appointment of a DPO will only be mandatory where the data controller is a public authority or the core activities of the data controller consist of processing operations which require: (i) regular and systematic monitoring of data subjects on a large scale; or (ii) processing on a large scale of sensitive personal data. For all other organisations, the appointment of a DPO will be voluntary.

This provides for a rather more grey area in relation to the DPO requirement. Whilst it is obvious that an organisation that processes a lot of sensitive personal data as part of its core business, such as a healthcare insurance provider, will need to engage a DPO to oversee data protection compliance, the situation is less clear in relation to other large organisations. Such organisations will process sensitive personal data on a large scale due to the amount of HR data they hold. However, would this processing be considered to be the "core activity" of the organisation in question? Commentators appear to be conflicted on this issue and so we may need to await future guidance.

Organisations that are going to be subject to the DPO requirement will need to start planning for the recruitment of such a person. The prescriptive qualification requirements of the DPO, which were proposed in earlier versions of the GDPR have been removed from the GDPR, although the text refers to a person with expert knowledge of data protection laws and practices. The Recitals to the GDPR also provide that the necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor.

The GDPR introduces a requirement for the DPO not to be dismissed or penalised by the data controller or processor for performing his tasks. This appears to grant the employee a protected status akin to trade union officials when carrying out their activities and leaves open the question of if/how an employee would enforce that right.

## SECURITY

With respect to data security, the GDPR is slightly more prescriptive than the Directive about what organisations need to have in place from a security perspective but not overly so, and certainly not as prescriptive as earlier drafts had suggested.

For example, Article 32 of the GDPR lists security measures such as:

- pseudonymisation and encryption of personal data;
- ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services;
- ability to restore the availability and access to data; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational security measures.

These are all basic measures that organisations should have in place in order to comply with the current legislation (even though the current legislation does not set out detailed requirements). However, the GDPR is no more prescriptive than outlined above, meaning that the legal requirements with respect to security are, perhaps surprisingly, not much more stringent than under the current Directive. However, it is worth noting that the security requirements are now legally extended to data processors as well as data controllers, putting processors on the hook for the first time for regulatory liability.

This is perhaps an area where we can hope and expect to see further guidance in the future from the new European Data Protection Board, required under Article 68 of the GDPR to publish guidance with respect to compliance with certain aspects of the GDPR. In the meantime, organisations will need to carry out an impact/risk assessment and review of existing security processes and procedures to determine whether they pass muster under the new rules.

Article 32 of the GDPR also provides that adherence to an approved code of conduct (pursuant to Article 40) or an approved certification mechanism (pursuant to Article 42) may be used as an element to demonstrate compliance with the security requirements set out. It therefore seems that the EU is hoping to encourage industry to work together to produce its own guidance and standards in this area (for further details regarding the code of conduct and certification mechanisms provided for in the GDPR, please see the paragraph "Guidance, Codes of Conduct and Certifications" below).

## DATA BREACHES

As expected, the GDPR introduces a requirement for data controllers to notify the regulatory authority of personal data breaches. Article 33 of the GDPR provides that data controllers shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the regulatory authority of a data breach. The only exception to this rule is in cases where the breach is "unlikely to result in a risk for the rights and freedoms of individuals".

The GDPR does not give any examples of types of breaches unlikely to result in a risk to the rights and freedoms of individuals. However, the Recitals give some insight as to what risks to rights and freedoms of individuals could include. They provide that a personal data breach may result in physical, material or moral damage to individuals such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other economic or social disadvantage to the individual concerned. Given this long list of possible consequences of data breaches, it seems likely that the exemption to the notification requirement will be interpreted very narrowly and data controllers should therefore exercise caution if looking to rely on it.

The GDPR goes in to further detail about the notification itself in Article 33. This Article provides that the notification must at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned;
- describe the likely consequences of the personal data breach;
- set out details of the data protection officer or other point of contact; and
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, to mitigate its possible adverse effects.

And it is not just the regulatory authority that has to be notified of data breaches. The GDPR also sets out a requirement for data controllers to notify individual data subjects of data breaches. Article 34 of the GDPR provides that, when the personal data breach is likely to result in a high risk of the rights and freedoms of individuals being compromised, the data controller shall notify the data subject without undue delay. The notification to the data subjects must be in clear and plain language and should contain much of the information also required to be given to the regulatory authority. There are some limited exceptions to the obligation to notify. However, the GDPR also provides that, if the controller has not already communicated the personal data breach to the data subject, the regulatory authority may nonetheless require it to do so.

The new data breach notification requirements are likely to place a significant additional compliance burden on data controllers. The short timeframe for notification required means that organisations are going to have to ensure they have processes in place to be able to act quickly in the event of a breach and be able to rapidly gather significant amounts of information about the breach. The de minimus threshold provided for notification seems likely to be construed very narrowly, meaning that even minor data breaches may need to be notified, placing additional strain not only on the data controllers but also the regulatory authorities themselves.

## SANCTIONS

The new sanctions, and specifically the level of fines provided for under the GDPR, have been the subject of much discussion. In the UK, organisations haven't had to unduly worry about data protection fines to date as these have been capped at £500,000. However, it has been clear from the outset of the GDPR process (back in January 2012), that the EU wished to increase the level of fines available for breaches of data protection law. That being said, the specific proposals for fines varied greatly between the EU institutions. The European Commission originally suggested fines of EUR 1 million, whilst the European Parliament increased this vastly to EUR 100 million or 5% of annual worldwide turnover.

The final text provides for a two-tier system of fines. Minor breaches of some of the more administrative provisions of the GDPR will be subject to a maximum fine of EUR 10 million or 2% of annual worldwide turnover (whichever is greater). More fundamental breaches of, for example, the data protection principles, will be subject to a higher fine of EUR 20 million or 4% of annual worldwide turnover (whichever is greater). It is worth noting that it is not clear from the wording of the GDPR whether the fines relating to a percentage of annual worldwide turnover would apply to group turnover or just the turnover of the legal entity in breach. The Recitals refer to the definition of undertaking in Articles 101 and 102 TFEU but this in itself is not determinative of the issue.

As a general comment, data protection is going to have to be something that all organisations pay closer attention to going forward. The way that the GDPR has fines and caps for failure to meet simple compliance measures, such as failing to appoint an EU representative, means that data protection compliance will have to be scrutinised at a level of detail that simply wasn't necessary before.

## GUIDANCE, CODES OF CONDUCT AND CERTIFICATIONS

The GDPR contains a number of mechanisms through which organisations can hope to get some guidance on interpretation of, and compliance with, the regulation.

Under the GDPR, a new European Data Protection Board will be established. Article 70 sets out the tasks of the European Data Protection Board, which include issuing guidelines, recommendations and best practices in relation to certain aspects of the GDPR.

The GDPR also envisages the establishment of codes of conduct and certification mechanisms which may be used by data controllers as an element to demonstrate compliance with certain aspects of the GDPR.

Pursuant to Article 40 of the GDPR, associations or other bodies representing categories of controllers or processors will be encouraged to draw up codes of conduct. Examples of areas which may be the subject of future codes of conduct include:

- fair and transparent data processing;
- legitimate interests;
- exercise of the rights of the data subjects;
- measures to ensure security of processing;
- notification of personal data breaches to the regulatory authority; and
- transfer of personal data to third countries.

The GDPR also provides for a certification mechanism under which controllers and processors can be certified by an accredited certification body with an appropriate level of data protection expertise. Certifications will be voluntary and used as a means of demonstrating compliance with the GDPR but will not reduce the responsibility of the controller or processor for actual compliance with the GDPR.

In these ways, it seems that the EU is hoping to encourage industry to work to produce its own guidance and standards for particulars area of compliance, although it remains to be seen whether or not any associations or other bodies will rise to the challenge of producing such guidance and whether this will prove helpful to data controllers or cause confusion if the codes of conduct are not consistent with either the European Data Protection Board's guidelines from time to time or the Information Commissioner's guidance.

## KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

**MIRIAM EVERETT**
PARTNER, LONDON

+44 20 7466 2378
Miriam.Everett@hsf.com

**NICK PANTLIN**
PARTNER, HEAD OF TMT & DIGITAL UK & EUROPE, LONDON
+44 20 7466 2570
Nick.Pantlin@hsf.com

**DUC TRAN**
OF COUNSEL, LONDON
+44 20 7466 2954
Duc.Tran@hsf.com

# LEGAL NOTICE