May 2017

DATA PRIVACY BRIEFING: Special Edition

Key Changes in the Data Privacy Legislation

The General Data Protection Regulation adopted on 27 April 2016 extends the scope of application of the EU data privacy rules, enhances individuals' rights to give them more control over their data, introduces a one-stop-shop mechanism for businesses throughout the EU and reduces bureaucracy. It will become effective on 25 May 2018 and will be directly applicable in EU Member States.

In This Issue

A. Towards Implementation of the General Data Protection Regulation

A significant overhaul of data privacy regulations, the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) was adopted by the EU's legislative bodies mid-last year, with the aim to provide a modernised, accountability-based compliance framework for data protection throughout Europe and is about to come into effect on 25 May 2018. Following the entry into force of the GDPR, Directive 95/46/EC and implementing national legislation (i.e., Greek Law 2472/1997) shall be repealed.

With just one year remaining for implementation, the present briefing aims to prepare and guide legal entities, by pointing out the key changes of the GDPR, in moving to compliance and making required changes to their programmes, internal processes and IT infrastructure.

B. Expanded Territorial Scope

A notable departure from the current legal framework is the extended territorial jurisdiction of the GDPR to cover all foreign entities processing data of EU residents.

The GDPR will apply to the processing of personal data by controllers/processors having an establishment in the EU (regardless of whether processing takes place within the EU), as well as to the processing of personal data of individuals within the EU by controllers/processors having an establishment outside the EU where the processing is related to:

1. the offering of goods or services (irrespective of whether connected to a payment); or

2. the monitoring of their behaviour so long as this behavior takes place within the EU.

The use of a language or a currency of an EU Member State, the possibility of ordering goods/services in that other language and reference to customers or users who are in the EU may constitute evidence that the controller envisages offering goods or services to EU data subjects. Monitoring behavior could occur where individuals are tracked on the internet by techniques for profiling purposes, particularly in order to take decisions concerning them or for analysing or predicting their personal preferences, behaviours and attitudes.
A foreign entity targeting or monitoring customers in the EU will become subject to the GDPR and will be required to nominate a representative to act on its behalf.

C. One-Stop Shop for Cross-Border Processing

From May 2018 and onwards, any processing carried out by a controller/processor with activities in more than one EU Member State will be supervised by the lead supervisory authority, i.e., the supervisory authority of the main establishment or of the single establishment of the controller/processor. This will enhance legal certainty and save money for businesses.
Each national supervisory authority shall retain jurisdiction over complaints and possible violations of the GDPR, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.

D. Higher Standards for Valid Consent

Under the GDPR, consent, as a justification for processing, will be harder to obtain. In particular, data subjects' consent must consist of a clear affirmative action in the sense that this must be freely given, specific, informed and unambiguous. The data controller must be able to demonstrate that the data subject has indeed consented. Silent consent, pre-ticked boxes or inactivity are excluded.
Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. Consent shall not be considered valid if bundled with other matters, or if it is a condition of performance of a contract (where processing is not necessary for the contract's performance), or if there is a clear power imbalance between the parties.
The requirement of parental consent for children (under the age of 16) to receive information society services is also introduced.
Data subjects must be able to withdraw their consent at any time.

E. Enhanced Data Subjects' Rights

One of the goals of the GDPR is to strengthen the rights of data subjects. The following rights are introduced:

1. **the right to be forgotten**, i.e., have their personal data erased, without undue delay, where these are no longer needed or relevant (in line with the Court of Justice's judgment in Google Spain);
2. **the right to object to profiling**, i.e., not be subjected to automated data profiling which produces legal effects; and
3. **the right to data portability**, enabling data subjects to obtain their data electronically and in a commonly used form and reuse their data for their own purposes and across different service providers.

Data portability will enable individuals to have more control over their data and is expected to benefit start-ups and smaller-sized businesses.

F. Data Protection by Design and by Default

The GDPR introduces the concepts of data protection by design and by default.
Data protection by design means that data processing activities must be designed, from the beginning, in such a way so as to ensure the privacy of the data. This involves the implementation of appropriate organisational and technical measures to ensure compliance with data protection principles and safeguard the data subjects' rights, such as data minimisation techniques, including pseudonymisation.
Data protection by default means that the data controller must ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed and that personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

G. Removal of Notification Requirement but Strict Data Breach Notification Obligation

Data controllers will no longer be required to notify or seek approval from their supervisory authority in many circumstances, but will be instead required, particularly for new technologies, to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. High risk processing requires prior consultation with the supervisory authority and the latter will have the power to provide written advice and use its enforcement powers where necessary.
In addition, data controllers will have the obligation to notify, without undue delay and, where feasible, within 72 hours, personal data breaches to the supervisory authority. If the

personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must also communicate the personal data breach to the data subjects without undue delay. This would practically mean that businesses will need to adopt internal procedures, including putting in place a data breach reporting and response plan, in order to be able to handle data breaches in the future.

H. Records of Processing Activities

Controllers/processors must keep a record of their processing activities, including specific information, in writing (it could also be in electronic form), which must be made available upon request of the supervisory authority. This obligation will not apply to a company with fewer than 250 employees, unless the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or it includes special categories of data or personal data relating to criminal convictions and offences.

I. Direct Obligations for Data Processors

Although data controllers will remain responsible for the acts of data processors, data processors will be subject to direct obligations and may be also held liable for non-compliance. Data processors will be required, inter alia, to designate a data protection officer where needed, appoint a representative when not established in the EU and notify the data controller without undue delay after becoming aware of a personal data breach.

J. International Data Transfers

No major departure from current rules is introduced by the GDPR. As expected, the GDPR makes express reference to binding corporate rules (BCR) as a basis for international data transfers (essentially reflecting what happens in practice).

K. Data Protection Officers

The GDPR makes it mandatory for data controllers/processors to designate a data protection officer in three specific cases:

1. where the processing is carried out by a public authority or body; or
2. where the core activities of the controller/processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale; or
3. where the core activities of the controller/processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

What is meant by core activities is the key operations necessary to achieve the controller's/processor's goals and should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller's/processor's activity (see Guidelines on Data Protection Officers, Article 29 Data Protection Working Party, 13 December 2016). As regards the term large scale, the preamble of the GDPR defines large-scale processing operations as ''operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk'', whereas the concept of monitoring the behaviour of data subjects encompasses all forms of online tracking and profiling, including for the purposes of behavioural advertising.

The role of the data protection officer is to:

1. inform and advise the controller/processor and the employees who carry out processing of their obligations pursuant to the GDPR;
2. monitor compliance with the GDPR and with the policies of the controller/processor in relation to the protection of personal data, including the assignment of responsibilities awareness-raising and training of staff involved in processing operations, and the related audits;
3. provide advice where requested as regards the data protection impact assessment and monitor its performance;
4. cooperate with the supervisory authority; and
5. act as the contact point for the supervisory authority on issues relating to processing, including prior consultation, and to consult, where appropriate, with regard to any other matter.

L. Higher Fines for Non-Compliance

The GDPR will significantly increase sanctions for non-compliance with the EU privacy rules and will enable supervisory authorities to impose fines as high as 4% of an undertaking's total worldwide annual turnover of the preceding financial year.

M. Ten Steps to Follow in Preparing for the GDPR

1. Raise awareness in your company that the rules will change and train your staff.
2. Document what personal data you process, their sources and recipients and keep detailed records of your processing activities.
3. Review and amend your privacy notices to align them with GDPR requirements.
4. Ensure compliance with individuals' rights, including the right to portability, and make sure you have procedures in

place to erase personal data.

5. Review your consent processes to ensure compliance with the GDPR. If children's data are involved, adopt mechanisms to verify the data subjects' age and obtain parental/guardian consent where required.
6. Ensure privacy by design and by default for new products, services and data processing activities.
7. Ensure you have procedures in place to detect, investigate and report personal data breaches.
8. Work on the implementation of data protection impact assessment processes and identify where this will be required.
9. Appoint a data protection officer, if necessary.
10. Determine the lead supervisory authority, if applicable.

Contacts

Marina Androulakakis
Associate
E mandroulakakis@bernitsaslaw.com

Tania Patsalia
Associate
E tpatsalia@bernitsaslaw.com