ALLEN & OVERY

The EU General Data Protection Regulation

2017

A new data protection landscape

After over four years of discussion, the new EU data protection framework has finally been adopted. It takes the form of a Regulation – the General Data Protection Regulation (GDPR). The GDPR will replace the current Directive and will be directly applicable in all Member States without the need for implementing national legislation. It will not apply until 25 May 2018. However, as it contains some onerous obligations, many of which will take time to prepare for, it will have an immediate impact.

Ever since the European Commission first proposed its text back in 2012, this legislation has attracted a huge amount of attention. It even appears to have been influencing decisions by the Court of Justice of the EU. Organisations across the EU and beyond have been frustrated by the increasing lack of harmonisation across the Member States, despite data flowing increasingly without boundaries. There was a growing desire to get the GDPR agreed quickly, even if that meant that some of the detail is left for later. The EU institutions have certainly stepped up to the plate. Adoption of the GDPR marks a milestone in data protection laws in the EU.

This note summarises some of the highlights in the GDPR.

"Now that the GDPR has been adopted, the shape of the EU's future data protection framework is clear and preparations for implementing the new Regulation should begin."

David Smith, special adviser to Allen & Overy

"…a major step towards a Digital Single Market."

Andrus Ansip, Vice President for the digital single market, European Commission

"The expanded territorial reach of the GDPR will offer a more balanced treatment between EU and non-EU data controllers."

Ahmed Baladi – Partner, Allen & Overy

What you need to know

EXPANDED TERRITORIAL REACH

The GDPR catches data controllers and processors outside the EU whose processing activities relate to the offering of goods or services (even if for free) to, or monitoring the behaviour (within the EU) of, EU data subjects. Many will need to appoint a representative in the EU.

The Recitals provide some helpful guidance. "Offering goods or services" is more than mere access to a website or email address, but might be evidenced by use of language or currency generally used in one or more Member States with the possibility of ordering goods/services there, and/or monitoring customers or users who are in EU. "Monitoring of behaviour" will occur, for example, where individuals are tracked on the internet by techniques which apply a profile to enable decisions to be made/predict personal preferences, etc.

This means in practice that a company outside the EU which is targeting consumers in the EU will be subject to the GDPR. This is not the case currently.

ACCOUNTABILITY AND PRIVACY BY DESIGN

The GDPR places onerous accountability obligations on data controllers to demonstrate compliance. This includes requiring them to: (i) maintain certain documentation, (ii) conduct a data protection impact assessment for more risky processing (DPAs should compile lists of what is caught), and (iii) implement data protection by design and by default, eg data minimisation.

DATA PROTECTION OFFICERS

In certain circumstances data controllers and processors must designate a Data Protection Officer (the DPO) as part of their accountability programme. The threshold is (i) processing is carried out by a public authority, (ii) the core activities of the controller or processor consist of processing which, by its nature, scope or purposes, requires regular and systematic monitoring of data subjects on a large scale, or (iii) the core activities consist of processing on a large scale of special categories of data.

The DPO will need sufficient expert knowledge. This will depend on the processing activities for which the officer will be responsible.

The DPO may be employed or under a service contract. A group of undertakings may appoint a single DPO (conditional on accessibility by all), as may certain groups of public authorities..

ROLE OF DATA PROCESSORS

One of the key changes in the GDPR is that data processors have direct obligations for the first time. These include an obligation to: maintain a written record of processing activities carried out on behalf of each controller; designate a data protection officer where required; appoint a representative (when not established in the EU) in certain circumstances; and notify the controller on becoming aware of a personal data breach without undue delay. The provisions on cross border transfers also apply to processors, and BCRs for processors are formally recognised.

The new status of data processors will likely impact how data protection matters are addressed in supply and other commercial agreements.

CONSENT

A data subject's consent to processing of their personal data must be as easy to withdraw as to give consent. Consent must be "explicit" for sensitive data. The data controller is required to be able to demonstrate that consent was given. Existing consents may still work, but only provided they meet the new conditions.

There has been much debate around whether consent provides a valid legal ground for processing where there is a significant imbalance between the data subject and data controller. The GDPR states that in assessing whether consent has been freely given, account shall be taken, for example, of whether the performance of a contract is made conditional on the consent to processing data that is not necessary to perform that contract. This may affect some e-commerce services, among others. In addition, Member States may provide more specific rules for use of consent in the employment context. The Recitals add that consent is not freely given if the data subject had no genuine and free choice or is unable to withdraw or refuse consent without detriment.

Where personal data is processed for direct marketing the data subject will have a right to object. This right will have to be explicitly brought to their attention.

Another topic of huge debate relates to parental consent being required for children to receive information society services. The compromise (that Member States can lower the age from 16 to 13) will result in a lack of harmonisation and companies who operate across several Member States generally choosing to meet the highest standard. The Recitals provide, however, that parental consent is not required in the context of preventative or counselling services offered directly to a child.

FAIR PROCESSING NOTICES

Data controllers must continue to provide transparent information to data subjects. This must be done at the time the personal data is obtained. However, existing forms of fair processing notice will have to be re-examined as the requirements in the GDPR are much more detailed than those in the current Directive. For example, the information to be provided is more comprehensive and must inform the data subject of certain of their rights (such as the ability to withdraw consent) and the period for which the data will be stored.

Controllers will need to consider their forms of fair processing notice with these new obligations in mind, and check in that they are providing the information in a clear way and in an easily accessible format.

DATA BREACH NOTIFICATION

Data controllers must notify most data breaches to the DPA. This must be done without undue delay and, where feasible, within 72 hours of awareness. A reasoned justification must be provided if this timeframe is not met. In some cases, the data controller must also notify the affected data subjects without undue delay.

The text looks burdensome on both data controllers and DPAs. However, in some sectors, organisations already have an obligation to notify data breaches.

Additionally, the UK ICO, for example, already expects to be informed about all "serious" breaches. The text also contains a welcome threshold. Notification does not need to be made to the DPA if the breach is unlikely to result in a risk to the rights and freedoms of individuals. The threshold for notification to data subjects is that there is likely to be a "high risk" to their rights and freedoms. While this may lessen the impact, all companies will have to adopt internal procedures for handling data breaches in any case.

"Many companies are re-examining their processes and procedures now in order to ensure compliance."

Nigel Parker – Partner, Allen & Overy

FINES

The GDPR establishes a tiered approach to penalties for breach which enables the DPAs to impose fines for some infringements of up to the higher of 4% of annual worldwide turnover and EUR20 million (eg breach of requirements relating to international transfers or the basic principles for processing, such as conditions for consent). Other specified infringements would attract a fine of up to the higher of 2% of annual worldwide turnover and EUR10m. A list of points to consider when imposing fines (such as the nature, gravity and duration of the infringement) is included.

The percentage applies to an "undertaking" and a last minute clarification in the Recitals adds that this is as defined in Articles 101 and 102 of the TFEU.

The increased fines are certainly attracting the attention of board level executives.

ONE-STOP-SHOP

When Viviane Reding introduced the Commission's proposed text, the 'One-Stop-Shop' was one of the key elements of her vision. The idea of a company which is established in many EU countries only having to deal with one lead DPA where it has its main establishment is attractive. However, the proposed mechanism was controversial and criticised for a range of reasons including over simplification and ceding too much control to other countries.

In order to enable individuals to have their cases dealt with locally, the agreed GDPR text contains a detailed regime with a Lead Authority and Concerned Authorities working together. It allows for local cases and urgent cases to be handled appropriately. How the One-Stop-Shop will work in practice, and whether it can work in such a way that it does not encourage forum shopping, remains to be seen.

REMOVAL OF NOTIFICATION REQUIREMENT

A welcome change for data controllers is the removal of the requirement to notify or seek approval from the DPA in many circumstances. The aim appears to be to alleviate the associated administrative and financial burden on data controllers but it will mean DPAs in some countries will need to replace this source of funding from elsewhere.

Instead of general notification, the policy is now to require data controllers to put in place effective procedures and mechanisms focussing on more high risk operations (eg involving new technologies) and carry out a data protection impact assessment to consider the likelihood and severity of the risk, particularly with large scale processing. The effort required, and the potential fines for getting it wrong, are likely to outweigh the benefit. In addition, the benefits of the removal of the notice requirement could be offset by the new requirement to consult the DPA in advance where a data impact assessment indicates that the processing would result in a high risk if measures are not taken to mitigate that risk. If the DPA feels that the processing would breach the GDPR, they may provide written advice and use their enforcement powers where necessary. This obligation creates uncertainty for data controllers as they will have to assess the outcome of the impact assessment and decide whether to consult.

NEW EUROPEAN DATA PROTECTION BOARD

An independent EDPB is to replace the Article 29 Working Party and will comprise the EDP Supervisor and the senior representatives of the national DPAs. Its obligations include issuing opinions and guidance, ensuring consistent application of the GDPR and reporting to the Commission. They also have a key role in the One-Stop-Shop mechanism.

BINDING CORPORATE RULES

The GDPR expressly recognises BCRs for controllers and processors as a means of legitimising intra-group international data transfers. The BCRs must be legally binding and apply to and be enforced by every member of the group of undertakings/enterprises engaged in a joint economic activity, including their employees. They must expressly confer enforceable rights on data subjects. The approach will be more streamlined with a clear list of requirements.

This method of compliance is seen by some as the "gold standard" and will become increasingly popular for intra-group transfers.

INTERNATIONAL TRANSFERS

Those who had hoped for a complete revamp in this area will be disappointed as the GDPR contains essentially the same toolkit. The process looks likely to be improved by the removal of the need for prior authorisation for transfers based on approved safeguards such as Commission or DPA approved contracts. However, the GDPR removes self-assessment as a basis for transfer: this is currently only used as a stand alone basis in a few Member States and is arguably a necessary sacrifice in order to achieve uniformity.

The consent derogation has also been amended: data exporters who rely on consent to move data outside the EU will need to look carefully at whether data subjects have been sufficiently informed of the risks of transfer.

The legitimate interests concept has been introduced as a new derogation, but its scope is limited. It may be used where the transfer is not repetitive, concerns only a number of data subjects, is necessary for compelling legitimate interests (not overridden by the rights of the data subject) and where the controller has assessed all the circumstances and adduced suitable safeguards. The DPA must also be informed. It is hard to see how this is useful in practice. It will be a relief to many that an outright ban on transfers to foreign regulators without DPA approval has not survived in the adopted text. The GDPR does nothing to resolve the issues around "safe harbour".

DATA SUBJECTS' RIGHTS

One of the main ambitions of the European Commission in proposing a new data protection framework was to bolster the rights of individuals. This desire is clearly reflected in the strengthened rights of data subjects. These include, for example, a right to require information about data being processed about themselves, access to the data in certain circumstances, and correction of data which is wrong. There is also a right to restrict certain processing and a right to object to their personal data being processed for direct marketing purposes. Individuals can also ask to receive back their personal data in a structured and commonly used format so that it can easily be transferred to another data controller (this is known as "data portability").

One of the rights that received the most attention, particularly following the CJEU decision in the Google v Spain case, is the "right to be forgotten" or "right of erasure" as it has become known. This allows individuals to require the data controller to erase their personal data without undue delay in certain situations, such as where they withdraw consent and no other legal ground for processing applies. Alongside this is an obligation to take reasonable steps to inform third parties that the data subject has requested erasure of any links to, or copies of, that data. This will often be difficult to manage in practice.

Note that the data controller must respond to these requests for information within a month, with a possibility to extent this period for particularly complex requests. Data controllers will need to put in place clear processes to enable them to meet these obligations. The information shall be provided free of charge unless the request is "manifestly unfounded or excessive".

What happens next?

On 4 May 2016, the General Data Protection Regulation, now numbered Regulation 2016/679, was published in the Official Journal of the EU. This means that we finally have certainty on the date from which it will apply. A period of 20 days had to pass following this publication, and the GDPR therefore entered into force on 25 May 2016. It will not "apply", however, until 25 May 2018. This allows much needed time to prepare.

Once the GDPR is in effect, the current Data Protection Directive 95/46/EC is repealed. As companies begin the process of moving to compliance with the new requirements, Member States will need to consider the impact on national legislation that implements the Directive.

MANY COMPANIES ARE NOW CONSIDERING THE FOLLOWING QUESTIONS:

What are the new obligations under the GDPR which will apply to their organisation?

What gaps exist between their existing state of compliance as against the standard required under the GDPR?

What changes should they make to achieve compliance with the GDPR, on what timetable, with what order of priority, and at what cost?

"The level of risk associated with the GDPR has catapulted data protection into the boardroom."

Jane Finlayson-Brown – Partner, Allen & Overy

Eight things you should be doing now to prepare

1. Prepare for data security breaches
   Put in place clear policies and well-practised procedures to ensure that you can react quickly to any data breach and notify in time where required.

2. Establish a framework for accountability
   Ensure that you have clear policies in place to prove that you meet the required standards. Establish a culture of monitoring, reviewing and assessing your data processing procedures, aiming to minimise data processing and retention of data, and building in safeguards. Check that your staff are trained to understand their obligations. Auditable privacy impact assessments will also need to be conducted to review any risky processing activities and steps taken to address specific concerns.

3. Embrace privacy by design
   Ensure that privacy is embedded into any new processing or product that is deployed. This needs to be thought about early in the process to enable a structured assessment and systematic validation. Implementing privacy by design can both demonstrate compliance and create competitive advantage.

4. Analyse the legal basis on which you use personal data
   Consider what data processing you undertake. Do you rely on data subject consent for example, or can you show that you have a legitimate interest in processing that data that is not overridden by the interests of the data subject? Companies often assume that they need to obtain the consent of data subjects to process their data. However, consent is just one of a number of different ways of legitimising processing activity and may not be the best (eg it can be withdrawn). If you do rely on obtaining consent, review whether your documents and forms of consent are adequate and check that consents are freely given, specific and informed. You will bear the burden of proof.

5. Check your privacy notices and policies
   The GDPR requires that information provided should be in clear and plain language. Your policies should be transparent and easily accessible.

6. Bear in mind the rights of data subjects
   Be prepared for data subjects to exercise their rights under the GDPR such as the right to data portability and the right to erasure. If you store personal data, consider the legitimate grounds for its retention – it will be your burden of proof to demonstrate that your legitimate grounds override the interests of the data subjects. You may also face individuals who have unrealistic expectations of their rights.

7. If you are a supplier to others, consider whether you have new obligations as a processor
   The GDPR imposes some direct obligations on processors which you will need to understand and build into your policies, procedures and contracts. You are also likely to find that your customers will wish to ensure that your services are compatible with the enhanced requirements of the Regulation. Consider whether your contractual documentation is adequate and, for existing contracts, check who bears the cost of making changes to the services as a result of the changes in laws or regulations. If you obtain data processing services from a third party, it is very important to determine and document your respective responsibilities.

8. Cross-border data transfers
   With any international data transfers, including intra-group transfers, it will be important to ensure that you have a legitimate basis for transferring personal data to jurisdictions that are not recognised as having adequate data protection regulation. This is not a new concern, but as failure to comply could attract a fine of up to the greater of EUR20m and 4% of annual worldwide turnover, the consequences of non-compliance could be severe. You may want to consider adopting binding corporate rules to facilitate intra-group transfers of data.

Contacts

Jane Finlayson-Brown
Partner – London
Tel +44 20 3088 3384
Mob +44 7767 674 407
jane.finlayson-brown@allenovery.com

Nigel Parker
Partner – London
Tel +44 20 3088 3136
Mob +44 7717 341 948
nigel.parker@allenovery.com

David Smith
Peerpoint Consultant – London
Tel +44 20 3088 6842
david.a.smith@allenovery.com

Charlotte Mullarkey
Counsel – London
Tel +44 20 3088 2404
Mob +44 7584 888 732
charlotte.mullarkey@allenovery.com

Krystyna Szczepanowska-Kozlowska
Partner – Poland
Tel +48 22 820 6176
krystyna.szczepanowska-kozlowska@allenovery.com

Justyna Ostrowska
Senior Associate – Poland
Tel +48 22 820 6172
justyna.ostrowska@allenovery.com

Tobias Neufeld
Partner – Düsseldorf
Tel +49 211 2806 7120
Mob +49 172 6865911
tobias.neufeld@allenovery.com

Prokop Verner
Counsel – Prague
Tel +420 222 107 140
Mob +420 724 262 415
prokop.verner@allenovery.com

Catherine Di Lorenzo
Senior Associate – Luxembourg
Tel +352 44 44 5 5129
Mob +352 621 372 410
catherine.dilorenzo@allenovery.com

Gary Cywie
Counsel – Luxembourg
Tel +352 44 44 5 5203
Mob +352 691 80 68 89
gary.cywie@allenovery.com

Antonio Martinez
Partner – Madrid
Tel +34 91 782 99 52
Mob +34 696 232 416
antonio.martinez@allenovery.com

Roxana Ionescu
Senior Associate – Bucharest
Tel +40 31 4057777
Mob +40 723 600 629
roxana.ionescu@rtprallenovery.com

Balazs Sahin-Toth
Counsel – Budapest
Tel +36 1 429 6003
Mob +36 30 212 1151
balazs.sahin-toth@allenovery.com

Filip Van Elsen
Partner – Antwerp
Tel +32 3 287 73 27
Mob +32 495 59 14 63
filip.vanelsen@allenovery.com

Zuzana Hecko
Senior Associate – Bratislava
Tel +421 2 5920 2438
Mob +421 917 105 777
zuzana.hecko@allenovery.com

Peter Van Dyck
Senior Associate – Brussels
Tel +32 2 780 25 12
Mob +32 494 82 18 47
peter.vandyck@allenovery.com

Anita Anand
Senior Associate – London
Rulefinder Cross-Border Data Transfer
Tel +44 20 3088 2831
Mob +44 7917 373 457
anita.anand@allenovery.com

"They are commercial, responsive, innovative and impressive to work with. They took the time to get to know our business and the results have been fantastic."

Chambers UK (Data Protection) 2015

GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,200 people, including some 530 partners, working in 44 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

Abu Dhabi
Amsterdam
Antwerp
Bangkok
Barcelona
Beijing
Belfast
Bratislava
Brussels
Bucharest (associated office)
Budapest
Casablanca
Doha
Dubai
Düsseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Istanbul
Jakarta (associated office)
Johannesburg
London
Luxembourg
Madrid
Milan
Moscow
Munich
New York
Paris
Perth
Prague
Riyadh (cooperation office)
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.
Yangon

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term **partner** is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings.