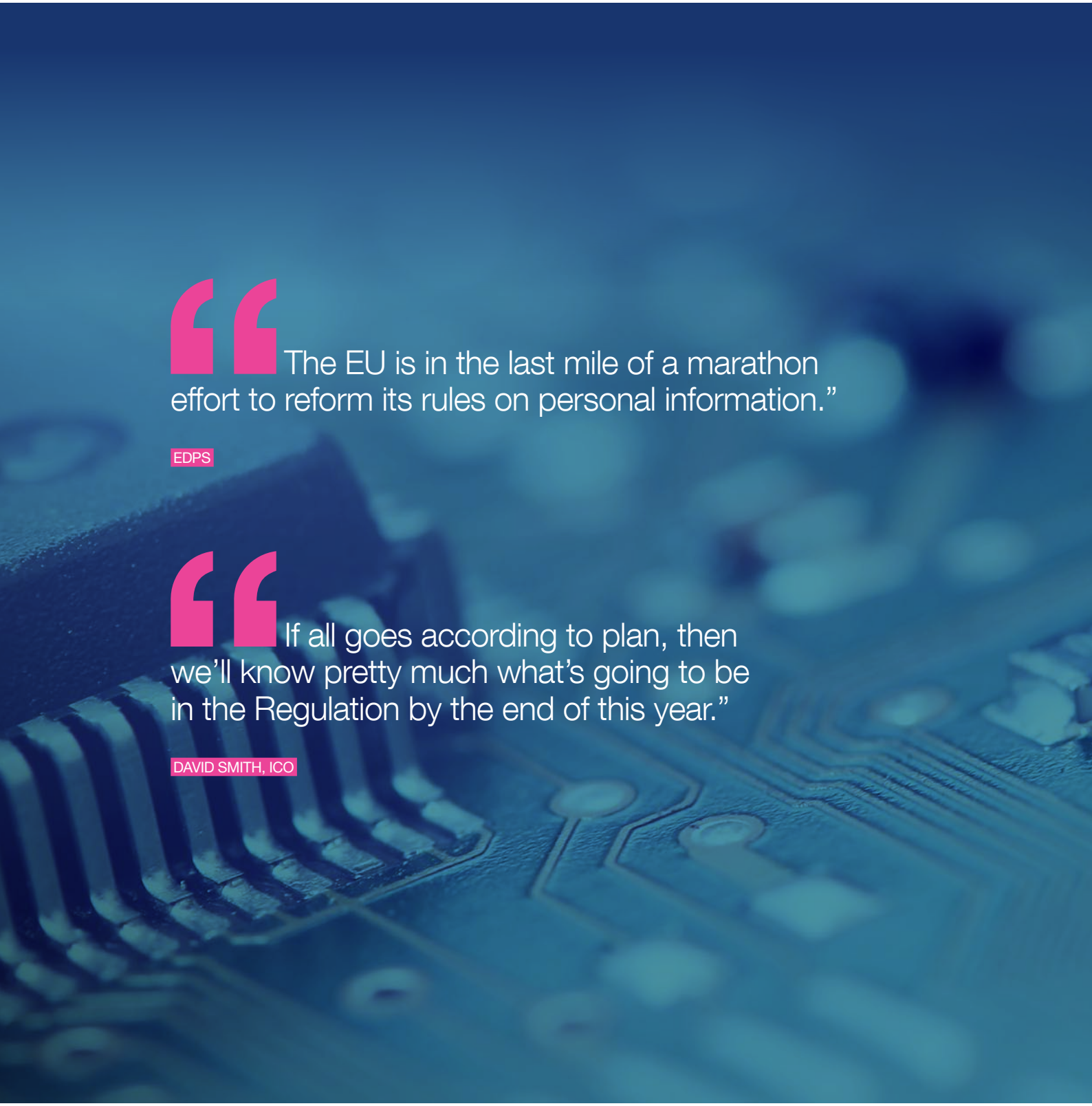
ALLEN & OVERY

What can we expect from the EU General Data Protection Regulation?

Autumn 2015



A new data protection landscape

After over three years of discussions at many levels, it is now clear that the proposed EU data protection framework will be revised, and that it will be in the form of a Regulation – the General Data Protection Regulation. The GDPR will replace the current Directive and will be directly applicable in all Member States without the need for implementing national legislation. It is currently under discussion in "trilogue" by the European Commission, the Parliament and the Council as they try to agree on a final text. Each institution has previously published its own form of the text, so we have a fair idea of which points might be harder to agree.

Ever since the European Commission first proposed their text back in 2012, this legislation has attracted a huge amount of attention. It even appears to be influencing decisions by the Court of Justice of the EU as they try to interpret EU law in an environment where many corporations are already starting to operate under the expected requirements of the new regime.

This response is hardly surprising. 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 is now a desire among many to get the GDPR agreed, even if this means leaving some of the detail for later. There is also a recognition that it is important to ensure that, whatever the result, we are at least left with the level of protection currently afforded by the Directive. DPAs are keen that the EU does not legislate for what they cannot fund.

This note summarises some highlights from the proposed GDPR, looking across the three draft texts. Further information and links to the relevant documents can be found on our dedicated website at: **www.allenovery.com/data-protection**

What you need to know

EXPANDED TERRITORIAL REACH

The GDPR will now catch data controllers outside the EU whose processing activities relate to the offering of goods or services (even if for free) to, or monitoring the behaviour of, EU data subjects. Many will need to appoint a representative in the EU. We understand that this provision was largely agreed in the second trilogue meeting.

The Recitals to some versions provide some helpful guidance on "monitoring of behaviour". This will occur 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 just targeting consumers in the EU would be subject to the GDPR. This is not the case currently.

DATA BREACH NOTIFICATION

Data controllers must notify any data breach to the DPA. It looks likely that this will have to be done without undue delay and, where feasible, within 72 hours of awareness. Two of the drafts require an explanation if this timeframe is not met. In some cases, the data controller must also notify the affected data subjects without undue delay.

The proposed text looks burdensome on both data controllers and DPAs. However, in some sectors, organisations already have an obligation to notify data breaches. Additionally, the ICO already expects to be informed about all "serious" breaches. If additional text proposed by the Council is agreed, we may see a welcome threshold for notification whereby the notification obligation would only apply to high risk breaches (eg where there is risk of fraud or damage to reputation). While this would lessen the impact on DPAs, all companies will have to adopt internal procedures for handling data breaches in any case.

CONSENT

A data subject's consent to processing of their personal data must be freely given, specific and informed, shown either by a statement or a clear affirmative action which signifies agreement to the processing. The Commission had proposed that this consent be "explicit" but the Council deleted this requirement which would be a helpful change. Consent can be withdrawn. The Commission and the Parliament impose the burden of proof on the data controller, and even in the Council's draft, the data controller is required to be "able to demonstrate unambiguous consent was given".

There is some difference in the texts around whether consent provides a valid legal ground for processing where there is a significant imbalance between the data subject and data controller. We expect this to remain in some form, even though it was removed in the Parliament and Council texts. This has particular relevance in the employment context and for consumer businesses.

Where personal data is processed for direct marketing the data subject will have a right to object and it looks likely that this right will have to be explicitly brought to their attention.

> "The level of risk associated with the GDPR has catapulted data protection into the boardroom."
>
> JANE FINLAYSON-BROWN

ACCOUNTABILITY AND PRIVACY BY DESIGN

The GDPR places onerous accountability obligations on the 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 (the Council suggesting that DPAs should compile lists of what is caught), and (iii) implement data protection by design and by default, e.g. data minimisation. Many organisations already go some way to meeting these requirements.

The CNIL's new PIA guides clearly anticipate implementation of the GDPR.

SANCTIONS

The GDPR establishes a tiered approach to penalties for breach which enables the DPAs to impose fines of up to 2-5% of annual worldwide turnover.

It is not yet clear whether this percentage applies to an entire corporate group but this is certainly possible, particularly when compared with the EU anti-trust regime. The ICO favours removal of the system of dividing different breaches of the Regulation into three tiers, each with different maximum fines, which it feels lacks flexibility and space for discretion.

We expect the principle of substantial fines to remain. This dramatic change is certainly already attracting the attention of board level executives.

ROLE OF DATA PROCESSORS

One of the key changes proposed by the GDPR is that data processors would have direct obligations. This includes implementing technical and organisational measures, notifying the controller without undue delay of data breaches and appointing a DPO (if required).

In several places the Council has removed direct obligations that the Commission had proposed for processors. It will be interesting to see the extent to which the final draft imposes obligations directly on data processors.

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

NIGEL PARKER

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 like the ICO will need to replace this source of funding from elsewhere.

Instead of notification, the policy now appears to be to require data controllers to maintain documentation on processing operations and conduct impact assessments for more risky processing. The effort required, and the potential fines for getting it wrong, are likely to outweigh the benefit.

INTERNATIONAL TRANSFERS

Those who had hoped for a complete revamp in this area were disappointed as all three texts contain essentially the same toolkit. In certain Member States the process looks likely to be improved by the proposed removal of the need for prior authorisation for transfers.

The legitimate interests concept has been introduced as a new derogation and applies to certain transfers which are not large scale or frequent. If this remains, in some countries it represents a useful broadening of the derogations. In others it is more restrictive (eg the removal of the ability to undertake self-assessment of adequacy, which had been a possible route in the UK).

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 some questions remain as to which entities within a corporate group must be included. This method of compliance will become increasingly popular for intra-group transfers.

The approach will be more streamlined with a clear list of requirements and one DPA taking the lead (subject to complying with a consistency mechanism).

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 criticized 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 Council has proposed a detailed regime with a Lead Authority and Concerned Authorities working together. We understand that the Commission broadly supports this proposal. How it will work in practice, and whether it can work in such a way that it does not encourage forum shopping, remains to be seen.

DATA PROTECTION OFFICERS

In certain circumstances data controllers and processors must designate a Data Protection Officer (the DPO) as part of their accountability programme. It is not clear what the threshold will be (eg number of people employed, number of data subjects affected or high risk processing being undertaken), but in reality many companies will need to appoint a DPO.

The DPO Officer will need sufficient expert knowledge. While this will depend on the processing activities for which the officer will be responsible, the ICO considers the list of qualities and functions proposed to be excessive and unrealistic.

The DPO may be employed or under a service contract. A group of undertakings may appoint a single DPO, as may certain groups of public authorities.

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, ensuring consistent application of the GDPR and reporting to the Commission. They would also have a key role in the Council's proposed one stop shop mechanism.

RIGHT TO BE FORGOTTEN

Now often called the right to erasure, individuals can require the erasure of their personal data (and possibly abstention from further dissemination) by the data controller in certain situations. A good example is where they withdraw consent and no other legal ground for processing applies. There is some difference in the three drafts but this concept looks set to stay, particularly since the recent CJEU decision in the *Google Spain* case.

Alongside this obligation is one to inform third parties that they should erase links and copies. We anticipate that this Commission proposal will be watered down in the final text.

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

What happens next?

We anticipate that the trilogue discussions should be completed by Spring 2016. However, it is possible that we may see drafts of particular sections of the GDPR that have been agreed before this. On final agreement, there will be a period of technical checking of the text and formal approvals. This may take several months. Only after that process is complete will the 2 year period run before the GDPR is in force. While this may seem a long time away, the organisations are already moving to compliance as many of the obligations (such as the accountability provisions) will take time to integrate.

8 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 (e.g. 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, informed and explicit. 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 proposed 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 2-5% 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

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

Quirine Tjeenk Willink
Counsel – Amsterdam
Tel +31 20 674 1352
Mob +31 622 938 323
quirine.tjeenkwillink@allenovery.com

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

Ahmed Baladi
Partner – Paris
Tel +33 1 40 06 53 42
Mob +33 622 747 582
ahmed.baladi@allenovery.com

Emmanuelle Bartoli
Associate – Paris
Tel +33 1 40 06 55 17
Mob +33 616 335 643
emmanuelle.bartoli@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

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

4,949 People
2,680 Lawyers
527 Partners
45 Offices
32 Countries

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

Lydia Mendola
Counsel – Milan
Tel +39 02 2904 9713
Mob +39 333 8745 910
lydia.mendola@allenovery.com

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

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

Magdalena Bartosik
Senior Associate – Warsaw
Tel +48 22 820 6131
Mob +48 606 431 012
magdalena.bartosik@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 5,000 people, including some 527 partners, working in 45 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 (associated office)
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Toronto
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.