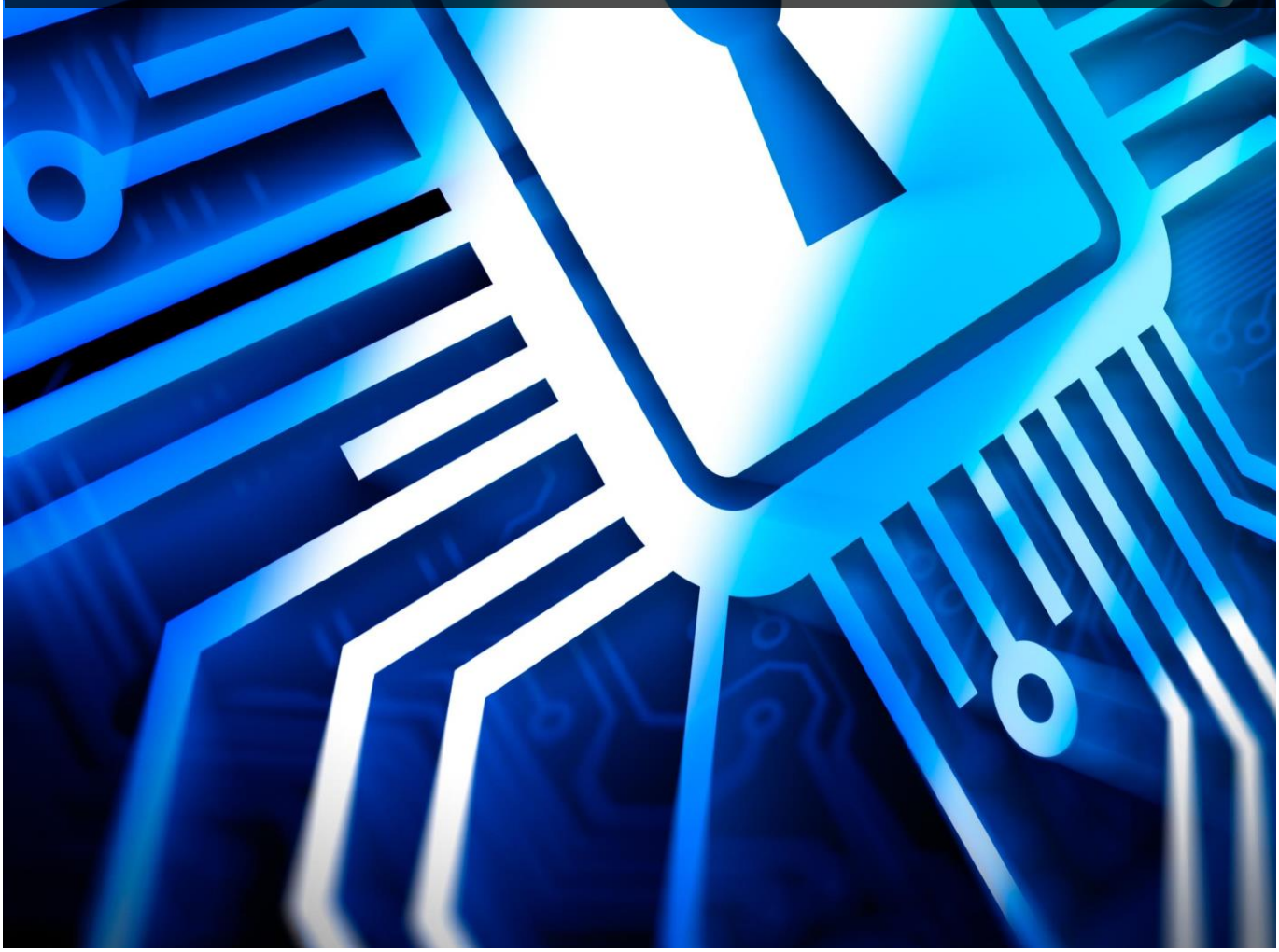
*Olswang LLP*

# GDPR is two years away: What does your board need to know?

OLSWANG



# GDPR is two years away: what does your board need to know?

Now that the GDPR has finally been agreed, how should businesses start to prepare? Olswang's Data Protection Team outline the Top 10 things your board needs to know.

*This article was first published in the January 2016 edition of Data Protection Law & Policy and is reproduced with kind permission.*

## GDPR AGREED AT LAST – NOW WHAT'S THE TIMETABLE?

In December, after almost four years of negotiation and intense lobbying, the EU institutions reached a compromise on the text of the General Data Protection Regulation. The final text - which is now is undergoing translation – is expected to be formally adopted in late Spring. Once the text is published in the Official Journal, probably around May 2016, the final countdown of 20 days and two years begins – so the Regulation should take direct effect in Member States in mid 2018. The GDPR represents not only a complete overhaul of data protection rules in Europe, but also a major gear-shift in terms of regulatory risk. Many businesses will have a lot of work to do to reach credible levels of compliance by 2018. What are the key practical areas for businesses to focus on, and what are the challenges likely to be?

## THE TOP 10 THINGS YOU NEED TO KNOW

### 1. A gear shift in risk

It is important to read GDPR through the lenses of the huge fines (up to 4% of global annual turnover) and other sanctions that it introduces. The current Data Protection Directive contains many (though not all) of the themes and requirements of GDPR, but crucially has nothing close to the new sanctions regime. Non-compliance with the Directive rarely led to serious fines or claims – and the big cases making headlines are the exception rather than the norm. Non-compliance with GDPR on the other hand could be terminal for your business.

### 2. Far more data is in scope

A wider definition of personal data brings a great deal more information into the regulated perimeter – so under the GDPR regime it will be even more important for business to minimise the personal information they collect. If you don't have a legal, legitimate reason to collect and process personal data, don't! Using aggregated anonymised data (falling outside GDPR's controls), or pseudonymous data (enjoying less stringent restrictions under GDPR) should be your first and second default options – personal data should only be collected and used where neither of these options are viable. Data by design and by default is not only a requirement under GDPR; it is a necessity to minimise your compliance exposure.

### 3. Wider applicable law test

The GDPR drops the "equipment/ means" test under the Directive and applies to the processing of personal data "in the context of the activities of an establishment of a controller or processor in the Union, regardless of whether the processing takes place in the Union or not" . It also expressly applies to controllers and processors not established in the EU, where the processing activities are related to either the offering of goods or services to data subjects in the EU (irrespective of whether payment is required for those goods or services) or the monitoring of their behaviour within the EU. Those non EU controllers and processors must designate a representative in the EU, as a point of contact for supervisory authorities and data subjects.

## 4. Processors are caught too

In one of the most fundamental changes to the current regime, the GDPR imposes a number of direct obligations and liabilities on processors. These include: the requirement to appoint a DPO (subject to same threshold as a controller); restrictions on sub processing; obligations to keep records of the processing carried out for a controller; cooperation with supervisory authorities; assessing and implementing appropriate security (with the controller) and notifying any breaches to the controller. Breaches of any of these provisions carry fines of up to 2% of global turnover. Processors are also subject to the restrictions on international transfers (fines of up to 4%). As well as now being directly exposed to fines, processors may be directly liable to data subjects for compensation if they breach the processor-specific obligations or act outside the controller's instructions. Fines are enforceable against non-EU/EEA processors through their EU-representative.

## 5. Greater accountability, governance - and resourcing

GDPR requires actual compliance rather than a few policies and tick box compliance. In practice this means completely transforming the way that your organisation deals with data governance – right across the business. This is not just a legal and compliance challenge; achieving readiness for GDPR will require much wider engagement right across an organisation to drive the change necessary. Business transformation takes time, budget and resource so organisations should start the exercise now, seeking a C-suite or senior management sponsor, appointing data champions across the business (for example in HR, IT, sales and marketing, supply chain) to drive best practice and spread the gospel of better data governance. There is a new focus on accountability: businesses must not only do the right thing, but be able to demonstrate they have complied with the data processing principles, for example through the use of Privacy Impact Assessments or showing compliance with Codes of Conduct or Certifications. Last but not least, there is the requirement for many controllers and processors to appoint a Data Protection Officer – a concept currently already in place in some member states, such as Germany and France – , meaning that baseline compliance costs could jump from a few hundred pounds to tens of thousands of pounds. The threshold for DPOs has been set much higher than was originally proposed and will now only apply to the public sector or controllers or processors engaged in regular and systematic monitoring of data subjects on a large scale. However, Member States have discretion to mandate DPOs in additional circumstances, so this threshold could vary across Europe.

## 6. The need to document your data processing (with care!)

GDPR is not a particularly green law, requiring controllers and processors to keep and make available to supervisory authorities very comprehensive records of data processing which in turn requires organisations to start work on detailed data mapping exercises to determine what data is collected, how and why, where it is stored, who has access to it and whether there is a legal justification to process it. This will take time and will almost certainly uncover data processing which is not compliant with the new GDPR requirements (or indeed, those of the current regime), so consideration should be taken as to how the review and report are prepared. Ideally your lawyers should be involved in the process to maximise the benefit of any legal privilege. You don't want a well-intended report to end up in the hands of your regulators or claimant lawyers in the event of a major incident.

## 7. Justifications for processing

Breach of the basic principles attracts the highest band (4%) of fines. GDPR will require organisations to take a much closer look at each purpose of data processing to ensure that there is a valid justification, particularly as the "bucket" justifications of consent and legitimate interests will be much narrower.

### 7.1 Consent

We were saved from what would have been a highly impractical requirement of explicit consent for all processing, but the new standard for consent is nevertheless more exacting. First, a controller must be able to demonstrate that consent was given. Second, transparency is key: consents given in written declarations which also cover other matters must be clearly distinguishable, and must be intelligible, easily accessible and in clear and plain language. Consent is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes – either by a statement or by a clear affirmative action. Consent may not be "freely given" if data controllers seek to make provision of a service dependent on consent to unnecessary personal data. Explicit consent will still be required for the processing of sensitive personal data ("special categories"). Consent will not provide a valid legal

ground where there is a clear imbalance between the data subject and the controller. So, what will valid consent look like in practice? We should expect to see far greater transparency, including the use of icons, more granular preferences and opt outs, and more just in time notifications. Cookie consent is a separate topic and we expect adjustments of the EU Cookie Directive (2002/58/EC as amended) in the near future.

### 7.2 Legitimate interests

Again, this condition survived, but is narrower than under the Directive. It remains a balancing test between the controller (or a third party's) legitimate interests and the interest or fundamental rights of and freedoms of the data subject – in particular where the data subject is a child. The privacy policy of a controller must inform about the legitimate interests that were basis for the balancing of interest. The recitals stress the need for careful case by case assessment, including the data subject's reasonable expectations. The recitals also offer some illustrations of when the condition might apply.

## 8. Enhanced data subject rights

Existing data subject rights are strengthened (subject access, rectification, rights in relation to automated decision making) and other rights are added (the Right To Erasure – a toned-down version of the Right To Be Forgotten, and data portability). Organisations will need to figure out technical and operational procedures to enable compliance with these rights – on pain of 4% fines.

## 9. Security requirements

The broad requirement for "appropriate technical and organisational measures" remains – but the GDPR fleshes out the requirement with factors to take into account, including pseudonymisation and encryption, the ability to ensure ongoing confidentiality, integrity, availability and resilience of systems and processing, the ability to restore availability and access in a timely manner, and processes for testing the effectiveness of security. The GDPR expressly provides for the use of approved codes of conduct or approved certification mechanisms as means to demonstrate compliance. Both controller and processor are responsible for implementing appropriate security.

## 10. Data breach notification requirements

Data breach notification is one of the most profound changes introduced by the GDPR. There are two strands: notification to regulators "without undue delay" but with an exacting 72 hour target, and communication to affected data subjects. Organisations have a great deal to do over the next couple of years to be able to detect and report breaches to supervisory authorities within the extremely tight deadline. This will require review of current technologies (firewalls, network monitoring and threat detection, logs), incident response procedures, crisis management procedures and policies. One of the biggest challenges for business is how to identify and escalate the most serious breaches quickly, given that data breach is now business as usual and occurs all the time. It is regrettable that GDPR has an extremely low threshold for breach notification ("likely to result in a risk for the rights and freedoms of individuals" in the case of notification to regulators, compared to "high risk" for communication to data subjects) and it is hoped that over the next couple of years guidance will be issued to help organisations and regulators standardise and streamline notification procedures so that time and resource can be freed up to deal with the most serious incidents quickly. Mishandling breach response can significantly increase losses suffered so organisations should also be practising and improving response with crisis teams and their lawyers – again, maintaining privilege and confidentiality rings is crucial.

# COMMENT - AND NEXT STEPS

GDPR was supposed to be about reducing red tape for businesses – instead, it has added to it. GDPR was also designed to harmonise rules throughout Europe – but there are plenty of provisions giving discretion to Member States to do things differently or impose stricter rules, including those regarding the child consent threshold, genetic and health data processing and appointment of data protection officers. The ambitious One Stop Shop principle

promised to simplify compliance for multinationals but has amounted to what appears to be a hugely bureaucratic co-operation procedure. Regrettably the consequence of achieving a relatively (!) speedy political compromise has resulted in a great deal more red tape and compliance cost for businesses – much of which has limited if any benefit to the data subjects that GDPR is intended to protect.

As the GDPR shifts data compliance to a higher gear, it is to be hoped that regulators will adopt pragmatic guidance and take a risk-based approach when it comes to enforcement. But given the scale of fines at stake and the rise of claims by individuals, businesses cannot afford to take a chance with the GDPR. The long road to GDPR compliance starts now, and it starts with buy-in from the top of your organisation, appropriate resourcing - and a serious stock take of your data assets.

**Andreas Splittgerber, Partner, Head of Data Protection Germany, Olswang LLP**

*"The concept for international data transfers to third countries outside the EU/EEA remains very similar under GDPR. Commission decisions that are in force now will also remain in force in the future. However, the Commission is called upon to review its decisions on a recurring basis. In addition to BCRs, the GDPR introduces Codes of Conducts that can be drawn up by, e.g., industry associations for a certain industry. This seems like a very attractive alternative to Safe Harbor (2.0) and EU Model Clauses, also for SMEs."*

**Ross McKean, Partner, International Head of Data Protection, Olswang LLP**

*"Mandatory data breach notification laws have transformed incident response in the US and have resulted in large fines, multiple class actions and numerous board level casualties. Organisations in Europe have much to learn from the US experience." GDPR introduces European wide mandatory data breach notification laws for the first time on pain of fines up to 2% of annual revenues with a risk of follow-on private actions for compensation by affected individuals. In addition to tackling the increasingly sophisticated cyber threat businesses will now have to build data breach infrastructure to be able to monitor, detect and respond to incidents within the exacting 72 hour deadline imposed by GDPR. Organisations should use the transition period in the run up to GDPR to develop and test incident response policies and to train cross-functional crisis teams. Lawyers will play a vital role in this exercise as maximising legal privilege is key to minimising losses arising from a major incident."*

**Sylvie Rousseau, Partner, Head of Data Protection Belgium and France, Olswang LLP**

*"Only time will tell whether the new principles will be fitted for the digital age and will resist for the next 20 years, as the principles of the Data Protection Directive (95/46/EC) have done. There are concerns that the implementation of the GDPR may prove more difficult for start-ups and small and medium enterprises (SMEs), which are less process oriented."*

This article was prepared with the help of Claire Walker, Head of Client Knowledge, Olswang LLP.

**Dr Andreas Splittgerber**
Partner
Munich
+49 89 206028-404

**Elle Todd**
Partner
London
+44 20 7067 3105

**Blanca Escribano**
Partner
Madrid
+34 91 187 1924

**Dan Tench**
Partner
London
+44 20 7067 3518

**Claire Walker**
Head of Client Knowledge
London
+44 20 7067 3174



Brussels
+32 2 647 4772

London
+44 20 7067 3000

Madrid
+34 91 187 1920

Munich
+49 89 206 028 400

Paris
+33 1 70 91 87 20

Singapore
+65 6720 8278

Thames Valley
+44 20 7071 7300


OLSWANG

Olswang:
Changing Business

www.olswang.com