SQUIRE PATTON BOGGS

GDPR

The European Union (EU) has been at the forefront of regulatory developments in data privacy and protection for the past two decades. The EU has adopted new legislation that will expand the existing privacy rights of EU residents while imposing a broad range of additional compliance obligations on businesses operating both in and outside the EU. *The new legislation – known as the General Data Protection Regulation (GDPR) – will become enforceable on May 25, 2018.*

Although May 2018 may seem to be a generous transition period, the scale of the changes imposed by the GDPR means that all organizations caught by the new rules will need to take steps to move toward compliance without delay.

Implications of the GDPR

In comparison to the existing EU data protection rules, the GDPR places greater emphasis on the obligations of *data controllers* (that is, those who determine when, how and for what purpose personal data is to be processed). It also imposes a significant number of new requirements directly on *data processors* (that is, those who process data on behalf of data controllers), which currently are subject only to the contractual obligations imposed on them by data controllers.

A new *accountability principle* will apply that will require companies that process EU personal data to create and maintain records demonstrating their compliance with the relevant GDPR requirements. In some cases, significant business process and even business model change will be required to meet the new obligations imposed by the GDPR. National Data Protection Authorities will have audit and investigatory powers to ensure that the requisite procedures are being followed.

The GDPR will reinforce and expand the data privacy rights of individuals in a number of important ways. At the same time, it will subject data controllers and processors that fail to comply with the GDPR requirements to potentially severe fines. The maximum penalties will be the higher of €20 million or 4% of annual worldwide turnover. The GDPR also establishes a right to compensation for aggrieved individuals and will enable them to lodge complaints through an organization, association or a not-for-profit body active in the field of data protection, which may represent them and receive compensation on their behalf.

Does the GDPR Affect My Company?

The GDPR will affect every business and public body that processes the personal data of EU residents, including:

Every employer in the EU.
All businesses that offer goods or services to individuals in the EU or that monitor their behavior, including companies that have no presence in the EU (meaning that the GDPR will have extraterritorial effect).
All businesses that process the personal data of EU individuals on behalf of other businesses (processors).

What Are the Key New Requirements?

The GDPR introduces a more stringent and prescriptive European data protection regime that will apply (in principle at least) on a more harmonized basis across the whole of the EU. Key changes include:

Direct liability for data processors – For the first time, organizations that process the personal data of other companies in the course of providing a service (such as cloud providers or website hosts) will have direct liability for breaches of the GDPR, including the risk of being fined. In addition, more extensive obligations will be required in processor agreements than are compulsory at present, and indemnities and limitation of liabilities will most likely become subject to renegotiation.

Data breach reporting – It will be mandatory for data controllers to notify, within 72 hours where feasible, the relevant Data Protection Authority about data breaches that may result in a risk to the rights and freedoms of individuals whose data is compromised; individuals may also need to be notified without delay if there is a "high risk" to their rights and freedoms.

New and expanded individual rights – The GDPR gives individuals a new "right to be forgotten" (have their personal data removed), a new right of data portability (have their personal data copied and transmitted to another organization for further use, including competitors) and enhanced data subject access rights. Individuals will also have expanded rights to object to processing, including an absolute right to object to direct marketing, which might have significant implications for businesses that rely on data analytics.

Limitations on profiling – There will be new limitations on data profiling, including a requirement to obtain prior consent to profiling, strict notice obligations regarding profiling and a duty to honor individuals' right to object to profiling, as noted above.

Appointment of Data Protection Officers (DPOs) – It will be mandatory for organizations, both data controllers and data processors alike, to appoint a DPO with expert knowledge in data protection reporting directly to the highest management levels, if (a) the organization is a public body, or (b) its core business requires regular and systematic monitoring of individuals on a large scale, or consists of the large-scale processing of sensitive personal data or criminal records.

Mandatory "data mapping" and documentation requirements – Controllers and processors will have to prepare and maintain comprehensive records of their processing activities, such as the purposes for processing, categories of data subjects and personal data, recipients of personal data, records of international transfers of data, records of data breach incidents, developing and maintaining privacy notices for each product line, storing verifiable consents, etc.

Consents – The GDPR sets out strict new requirements for obtaining valid and verifiable consents for the processing of personal data from data subjects, where consent is used as the basis for processing EU personal data.

Enhanced Privacy notices – The GDPR sets out specific information to be included in privacy notices and requires individuals to be given clear information as to what is done with their data in an easily accessible form.

Data protection Impact Assessments – These will be mandatory before undertaking "high risk" processing, including profiling or heavy use of sensitive personal data (such as health records). Further guidance will be provided by national regulators as to what constitutes "high risk" processing, but the scope is expected to be relatively broad.

Transfers outside the EU – Non-compliance with the prohibition against sending personal data to jurisdictions without adequate levels of data protection will attract very high fines. It is more important than ever for companies to confirm that their international transfers of employee and customer data are carried out pursuant to one of the methods approved by the European Commission (EU Standard Clauses, EU-U.S. Privacy Shield, Binding Corporate Rules, etc.).

What Will the Impact of Brexit Be?

The UK's formal withdrawal from the EU is unlikely to be completed before the GDPR becomes enforceable in May 2018. This means that UK businesses must prepare to comply with the GDPR as of that date. If the UK becomes a member of the EEA post-Brexit, the GDPR will still apply. Otherwise, the UK is likely to choose to continue to be subject to the GDPR, or to implement a mirror regime, in order to facilitate trade with the EU and many other parts of the world that value data privacy.

How We Are Helping Businesses Address the New GDPR Requirements

Our Data Privacy & Cybersecurity team is well-placed to help your organization understand and implement practical approaches to meet the challenges and opportunities that the GDPR presents.

Our data protection experts around the world (including in key EU Member States) have comprehensive knowledge of the changing European data protection landscape and are already advising SMEs, multinational companies and global organizations on their new EU data privacy obligations.

We can help your organization become GDPR-ready by working with you on the following initiatives:

Providing comprehensive advice and support in bringing products, services, processes and systems into compliance by 2018, including:

- Implementing data mapping processes as required by the GDPR and helping identify compliance gaps – we have developed comprehensive mapping documents for you to use.
- Evaluating whether processing qualifies as "high risk" and carrying out data protection impact assessments.
- Drafting and future-proofing new agreements, including reviewing how liability for infringements is allocated – and consider whether existing contracts need to be updated.
- Helping you assess the adequacy of the security arrangements of your service provider processors, including providing security compliance checklists.
- Reviewing and redrafting privacy notices to include the new mandatory information required by the GDPR.
- Putting in place mechanisms for obtaining explicit data subject consents, of particular importance to organizations engaged in tracking, behavioral advertising or any other form of profiling.
- Assisting you to create a robust data breach response plan that will help your organization meet the 72-hour notification deadline – our extensive experience with data breach preparedness, response and notification procedures in the US and the UK means we are well-positioned to assist clients with preparations for the even more aggressive reporting requirements that will apply under the GDPR.
- Developing data subject access systems that will enable your organization to respond to requests in the manner and within the timeframe stipulated in the GDPR.
- Assisting you in identifying your main establishment for the purpose of the GDPR.
- Advising on compliance with new mandatory DPO requirements.
- Where businesses are established outside the EU, assisting you in evaluating whether you are caught by the GDPR.
- Assisting you in reviewing your international transfers and consider what the most efficient transfer solution would be.

Working with data processors to risk-assess their operations in light of their new exposure to direct liability for breaches.

Advising on the EU-U.S. Privacy Shield, EU Standard Contractual Clauses, Binding Corporate Rules (for controllers and processors) and other measures available to legitimize transfers of personal data to (and remote access from) points outside of the EU.

Helping you develop good working relations with national data protection authorities, assisting with mandatory and voluntary consultation with them, responding to audit requests and providing representation as needed.

Providing education and training on EU data protection issues for all stakeholders in your organization.

Advising on the evolving Brexit implications, "one-stop shop" and other strategic jurisdictional issues.

Assisting with advocacy on policy issues before national and EU Data Protection Authorities to help influence their thinking on interpretation of the GDPR where this is of importance in a particular industry or sector.

Advising industry groups on the development and approval of new certification programs and codes of conduct.

Companies doing business in and with the EU should take note that GDPR is not simply a new check-the-book exercise. Compliance will require a concerted internal effort to interpret and apply the new rules. For further information on how our experienced data protection lawyers can help support you in this effort, please contact any member of our Data Privacy & Cybersecurity team listed on the following page.

Contacts

Global Data Privacy & Cybersecurity Team Leaders

Ann LaFrance
T +44 207 655 1752
E ann.lafrance@squirepb.com

Robin B. Campbell
T +1 202 457 6409
E robin.campbell@squirepb.com

Australia

Margie Tannock
T +61 8 9429 7456
E margie.tannock@squirepb.com

Belgium

Anthony Bochon
T +322 627 76 28
E anthony.bochon@squirepb.com

Monika Kuschewsky
T +322 627 11 11
E monika.kuschewsky@squirepb.com

China

Dan Roules
T +86 21 6103 6309
E daniel.roules@squirepb.com

Czech Republic

Hana Gawlasová
T +420 221 66 2240
E hana.gawlasova@squirepb.com

France

Stéphanie Faber
T +33 1 5383 7583
E stephanie.faber@squirepb.com

Germany

Annette Demmel
T +49 30 7261 68 108
E annette.demmel@squirepb.com

Andreas Fillmann
T +49 69 1739 24 23
E andreas.fillmann@squirepb.com

Jörg Staudenmayer
T +49 7031 439 9632
E jorg.staudenmayer@squirepb.com

Hong Kong

Nicholas Chan
T +852 2103 0388
E nick.chan@squirepb.com

Hungary

Ákos Eros
T +36 14 287 155
E akos.eros@squirepb.com

Csaba Vári
T +36 14 287 159
E csaba.vari@squirepb.com

Japan

Takujiro Urabe
T +81 3 5774 1800
E takujiro.urabe@squirepb.com

Scott Warren
T +81 3 5774 1800
E scott.warren@squirepb.com

Poland

Edyta Dubikowska
T +48 22 395 5526
E edyta.dubikowska@squirepb.com

Eligiusz J. Krzesniak
T +48 22 395 5524
E eligiusz.krzesniak@squirepb.com

Ewelina Witek
T +48 22 395 5565
E ewelina.witek@squirepb.com

Russia

Irina P. Golovanova
T +7 495 258 5253
E irina.golovanova@squirepb.com

Sergey A. Treshchev
T +7 495 258 5250
E sergey.treshchev@squirepb.com

Slovak Republic

Tatiana Prokopová
T +421 2 5930 3433
E tatiana.prokopova@squirepb.com

Spain

Fernando González
T +34 91 426 4843
E fernando.gonzalez@squirepb.com

UK

Aline Doussin
T 44 207 655 1146
E aline.doussin@squirepb.com

Caroline Egan
T +44 121 222 3386
E caroline.egan@squirepb.com

Francesca Fellowes
T +44 113 284 7459
E francesca.fellowes@squirepb.com

Asel Ibraimova
T +44 227 655 1208
E asel.ibraimova@squirepb.com

Stuart James
T +44 121 222 3645
E stuart.james@squirepb.com

Andrew J. Wilkinson
T +44 207 655 1783
E andrew.wilkinson@squirepb.com

Ukraine

Peter Z. Teluk
T +380 44 591 3154
E peter.teluk@squirepb.com

US

Paul C. Besozzi
T +1 202 457 5292
E paul.besozzi@squirepb.com

Elliot Golding
T +1 202 457 6407
E elliot.golding@squirepb.com

Clark K. Ervin
T +1 202 457 5234
E clark.ervin@squirepb.com

Gretchen Ramos
T +1 415 743 2576
E gretchen.ramos@squirepb.com

Philip Zender
T +1 415 393 9827
E philip.zender@squirepb.com