SQUIRE PATTON BOGGS

GDPR Compliance
How to Meet the 25 May 2018 Deadline

Have You Set Your Compliance Clock?

The EU General Data Protection Regulation ("GDPR") applies to many EU businesses as well as to companies without an EU presence if they process EU personal data. The scale of the changes imposed by the GDPR is significant and organizations caught by the new rules need to take steps now to ensure full compliance by May 2018.

This document aims to highlight the main steps required to comply, explain why they matter and provide average time estimates for each step of this process.

Our global Data Privacy & Cybersecurity team will help you develop and implement a compliance plan and timetable suitable for your organization.

Stage I

Step 1: Data Mapping

3-6 Months +

Action

Identify and map your data processing activities, including data flows and use cases in order to create a comprehensive record of activities.

Why?

GDPR requires you to keep detailed records of data processing activities. These records can be used to assess the compliance steps required by the business going forward and respond quickly to data breaches and to individuals who request their own data.

Step 2: Privacy Governance/ Data Protection Officer

1-3 Months

Action

Assess whether you are required to appoint a Data Protection Officer (DPO) and if so, recruit a professional who meets the GDPR criteria. Irrespective of the legal requirement, review and, if necessary, improve the corporate governance policies and structure to ensure that they are effective to achieve reasonable compliance throughout the business.

Why?

Appointment of a DPO is mandatory for some businesses. Robust data governance is, in any event, key to fulfilling the accountability obligation of all organizations.

Stage II

Step 3: Data Sharing — 6 Months +

Action

Identify any data sharing with third parties, determine the role of those parties and put appropriate safeguards in place. This may require the execution of new or revision of existing agreements.

Why?

GDPR imposes mandatory content for certain agreements and requires the clear assignment of roles and responsibilities.

Step 4: Justification for Processing — 6 Months

Action

Review or establish legal bases for processing, at least for key use cases. Plan and implement remedial action to fill any compliance gaps.

Why?

GDPR requires that all data processing has a legal basis, such as consent, contract and balance of interests, etc. and makes usage more difficult. GDPR also contains restrictions/ additional obligations relating to the use of automated processing, including profiling.

Step 5: Privacy Notices and Consents — 2-3 Months

Action

Review and amend all privacy notices, consent forms and related processes in order to comply with the GDPR.

Why?

The GDPR imposes additional minimum content for privacy notices. It also imposes stricter consent requirements.

Stage III

Step 6: Data Protection Impact Assessments

3 Months

Action

Assess whether the business carries out any "high risk" processing under the GDPR. If so, carry out a Data Protection Impact Assessment (DPIA) and, if necessary, consult with your supervisory authority.

Why?

DPIAs must be carried out in relation to all "high risk" processing and consultation with supervisory authorities may be required in certain circumstances.

Step 7: Policies

6 Months

Action

Review and supplement the company's existing suite of policies and processes dealing with data protection, including those dealing with data retention and integrity, such as data accuracy and relevance.

Why?

The GDPR imposes stricter obligations to keep data accurate, proportionate and no longer than necessary.

Step 8: Individuals' Rights

3 Months

Action

Identify the new individual rights provided by the GDPR and establish procedures for dealing with them. Review the procedures in place in order to comply with the expanded existing rights and revise processes, where required.

Why?

GDPR extends existing rights and introduces new rights for individuals, such as the right of data portability and erasure.

Step 9: Privacy by Design and Default

6-9 Months

Action

Review or establish procedures for ensuring that GDPR compliance is embedded in all applications and processes that involve personal data from the start. Default settings must comply with the GDPR.

Why?

Compliance must be integrated into all processes and applications that involve the use of personal data, and default settings must comply with the GDPR, including data minimization.

Stage IV

Step 10: International Data Transfers

2-3 Months

Action

Identify and review the data transfer mechanisms in place in order to comply with the GDPR. Fill any gaps, including entering into Standard Contractual Clauses with service providers and group companies, and evaluate the use of Binding Corporate Rules ("BCRs").

Why?

The GDPR retains the current requirement to have adequate measures in place when transferring personal data outside the EEA, but sanctions for non-compliance are substantially increased.

Step 11: Data Security and Breach Management Process

3-6 Months

Action

Review the data security measures in place to ensure they are sufficient and to assess whether the specific measures referred to in the GDPR are (or should be) in place. Review or establish an effective Data Breach Response Plan.

Why?

The GDPR implements stricter requirements regarding appropriate technical and organizational data security measures. It also requires data breaches involving risk to individuals to be reported to supervisory authorities without delay and within 72 hours (unless a longer period can be justified); affected individuals must also be notified if the breach is high risk.

Stage V

Step 12: Roll-Out of Compliance Tools and Staff Training

6 Months +

Action

Roll-out amended and new privacy notices and consent forms. Publish new and revised policies and procedures and conduct training of key personnel on GDPR compliance.

Sampling of Additional Services Offered by our Global Team

- GDPR Compliance
- BCRs
- Privacy Shield
- Data Transfer Agreements
- Cross-border Investigations
- Data Breach Planning and Response
- Cybersecurity Preparedness and Crisis Management
- IoT
- Website Review
- Consents
- Privacy Impact Assessments
- Privacy Policies
- Employee Privacy
- Whistleblower Hotlines
- Training
- Strategic Policy, Legal and Regulatory Support
- Privacy and Cybersecurity Litigation

Global Data Privacy & Cybersecurity Team Contacts

SQUIRE PATTON BOGGS

GDPR Compliance
How to Meet the 25 May 2018 Deadline

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

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

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