Baker & McKenzie's GDPR Game Plan

EU General Data Protection Regulation in 13 Game Changers

What businesses need to know and do to prepare

The EU General Data Protection Regulation ('GDPR') will replace the current Data Protection Directive 95/46/EC ('Directive') and will be directly applicable (most likely as of May 2018) in all EU Member States without need for implementing national laws. Businesses should already start adapting their data protection compliance programs, processes and infrastructure to prepare for the following Game Changers.

1. **Expanded Scope and One-Stop-Shop:** The GDPR applies to the processing of personal data by data controllers and processors established in the EU, as well as by controllers and processors outside the EU where their processing activities relate to the offering of goods or services (even for free) to data subjects within the EU, or to the monitoring of their behaviour. The supervisory authority in the jurisdiction of the main or single establishment of the controller/ processor will be the lead authority for cross-border processing (subject to derogations). ***►To do: Assess whether, as non-EU controller or processor, you will fall within the scope of the GDPR. Determine where your main establishment might be located based on your data processing activities.***

2. **Enhanced Rights of Data Subjects:** The GDPR includes a wide range of existing and new rights for data subjects. Amongst these are the right to data portability (right to obtain a copy of one's personal data from the controller and have them transferred to another controller), right to erasure (or 'right to be forgotten'), right to restriction of processing, right to object to certain processing activities (profiling) and to automated processing decisions. Controllers will also be required to provide significantly more information to data subjects about their processing activities. Click here for a detailed analysis. ***►To do: Implement appropriate processes and infrastructure to be able to address data subjects' rights and requests and update your privacy notices.***

3. **Profiling Restrictions:** Data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. Individuals will also have an express right to 'opt out' of profiling and automated processing in a wide range of situations. ***►To do: If you are engaging in profiling activities, consider how best to implement appropriate consent mechanisms.***

4. **Consent:** Consent is retained as a processing condition but the GDPR is more prescriptive than the Directive when it comes to the conditions for obtaining valid consent. The key change is that consent will require a statement or clear affirmative action of the data subject. Silence, pre-ticked boxes and inactivity will not be sufficient. The GDPR clarifies cases where consent will not be freely given (e.g., no genuine choice to refuse, clear imbalance between the data subject and controller). Data subjects must be informed of their right to withdraw consent. Click here for a detailed analysis. ***►To do: Identify your processing activities that are legitimised through consent. Consider whether other (potentially safer) processing conditions or legal justifications could be relied on. If and when relying on consent, ensure to adapt the way you collect consent in light of the new requirements.***

5. **Data Processors:** The GDPR imposes compliance obligations directly on processors, such as implementing security measures, notifying the data controller of data breaches, appointing a DPO (if applicable), maintaining records of processing activities, etc. Processors will be directly liable in case of non-compliance and may be subject to direct enforcement action. Controllers and processors will be required to enter into detailed processing agreements or renegotiate existing ones. Click here for a detailed analysis. ***►To do: As controller, carefully review the processor selection process und update your processor agreements. As processor, identify whether you fall within the scope of the GDPR, understand your new obligations and assess operational impact.***

6. **Data Mapping:** Controllers and processors will have to maintain records of processing activities. Detailed information must be kept and provided to supervisory authorities upon request. Click here for a detailed analysis. ***►To do: Ensure you understand and document what personal data you actually hold, process and transfer and how such data "flows" around your organisation.***

7. **Data Protection by Design and by Default:** These concepts are codified in the GDPR and require controllers to ensure that individuals' privacy is considered from the outset of each new processing, product, service or application, and that, by default, only minimum amounts of personal data as necessary for specific purposes are collected and processed . ► ***To do: Implement measures, such as pseudonymisation or data minimisation designed to implement data protection principles from the outset of any project.***

8. **Data Protection Impact Assessments ('DPIAs'):** Controllers will be required to perform a DPIA where the processing of personal data (particularly when using new technologies) is likely to result in a high risk to the rights and freedoms of individuals. DPIAs will particularly be required in cases of (i) an evaluation of personal aspects based on automated data processing including profiling, (ii) processing on a large scale of special categories of data, or (iii) systematic monitoring of a publicly accessible area. ►***To do: Make DPIAs part of the standard procedure for all processing operations so that they are easier to implement as an everyday task. Train staff on DPIAs and document them appropriately.***

9. **Accountability:** Businesses will have to ensure through appropriate technical and organisational measures compliance with the requirements of the GDPR and be able to objectively demonstrate such compliance. ► ***To do: Build a framework and internal compliance structure (ideally in the form of a comprehensive privacy compliance program) to ensure compliance with the GDPR requirements. Put appropriate policies and procedures in place to demonstrate compliance.***

10. **Data Protection Officer ("DPO"):** Certain private and most public sector organisations will be required to appoint a DPO to oversee their data processing operations. A DPO will be required where (i) the processing is carried out by a public authority or body, (ii) the core activities of the controller or processor consist of processing which requires regular and systematic monitoring of data subjects on a large scale, (iii) the core activities consist of processing special categories of data on a large scale, or (iv) required by Member State law. Click here for a detailed analysis. ►***To do: Consider who to hire or appoint as a DPO, taking into account that DPOs are required to have expert knowledge of data protection law and practices. A group of undertakings may appoint a single DPO provided the latter is easily accessible from each entity.***

11. **Overhauled Data Transfers Rules:** The GDPR retains the cross-border data transfer rules of the Directive, but adds new ones such as certification mechanisms and codes of conduct, as well as a new very limited derogation for occasional transfers based on legitimate interest. Country-specific authorisation processes will no longer be needed (with some exceptions). BCRs are formally recognised in the GDPR. Click here for a detailed analysis. ►***To do: Establish a comprehensive inventory of your cross-border data flows and review/ update your cross-border transfer strategy in light of the new rules stemming from the GDPR, jurisprudence (i.e., Schrems) and the incoming EU - U.S. Privacy Shield.***

12. **Data Breach Notification:** Controllers will have to report data breaches to the relevant supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of the breach (unless the breach is unlikely to result in a risk for data subjects' rights and freedoms). A proper justification shall accompany the notification if it is not made within 72 hours. Affected data subjects must be notified of a breach without undue delay if the breach is likely to result in a "high risk" for their rights or freedoms. Click here for a detailed analysis. ►***To do: Prepare for security breaches now with internal guidelines and policies on how to react and who to notify. Implement employee training to prevent and handle breaches.***

13. **Enforcement & Sanctions:** The GDPR will harmonise the tasks and powers of supervisory authorities and significantly increase fines. For major infringements (such as failure to comply with cross-border transfer rules or to obtain adequate consents) fines can be up to 20 million EUR or, in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year (whichever is higher). Click here for a detailed analysis. ►***To do: Implement appropriate structures, processes and policies (including auditing and staff training) to be able to ensure and demonstrate compliance with all obligations under the GDPR.***

North America

Chicago

Brian Hengesbaugh
Partner
+1 312 861 3077
brian.hengesbaugh@bakermckenzie.com

Palo Alto

Lothar Determann
Partner
+650 856 5533
lothar.determann@bakermckenzie.com

Toronto

Theo Ling
Partner
+416 865 6954
theodore.ling@bakermckenzie.com

EMEA

Amsterdam

Wouter Seinen
Partner
+31 20 551 7161
wouter.seinen@bakermckenzie.com

Brussels

Elisabeth Dehareng
Partner
+322 639 3705
elisabeth.dehareng@bakermckenzie.com

Brussels

Daniel Fesler
Partner
+322 639 3658
daniel.fesler@bakermckenzie.com

London

Dyann Heward-Mills
Partner
+44 20 7919 1269
dyann.heward-mills@bakermckenzie.com

Madrid

Raul Rubio
Partner
+34 91 436 6639
raul.rubio@bakermckenzie.com

Milan

Francesca Gaudino
Partner
+39 0 2762 31452
francesca.gaudino@bakermckenzie.com

Munich

Daniel Krone
Partner
+49 89 5 52 38 156
daniel.krone@bakermckenzie.com

Munich

Michael Schmidl
Partner
+49 89 5 52 38 155
michael.schmidl@bakermckenzie.com

Munich

Julia Wendler
Partner, Munich
+49 89 552 38242
julia.wendler@bakermckenzie.com

Paris

Denise Lebeau-Marianna
Partner
+33 1 4417 5333
denise.lebeau-marianna@bakermckenzie.com

Zurich

Nicolas Passadelis
Partner
+41 443 841 209
nicolas.passadelis@bakermckenzie.com

Asia Pacific

Sydney

Anne-Marie Allgrove
Partner
+61 2 8922 5274
anne-marie.allgrove@bakermckenzie.com

Latin America

Bogota

Carolina Pardo
Partner
+57 1 634 1559
carolina.pardo@bakermckenzie.com

Buenos Aires

Guillermo Cervio
Partner
+54 11 4310 2223
guillermo.cervio@bakermckenzie.com

Lima

Teresa Tovar
Partner
+51 1 618 8552
teresa.tovar@bakermckenzie.com

Sao Paulo

Flavia Rebello
Partner
+55 11 3048 6851
flavia.rebello@bakermckenzie.com