Baker McKenzie.

EU General Data Protection Regulation in 13 Game Changers

March 2018

Contents

The General Data Protection Regulation – Finally Here!

At the time of writing, it has been close to two years since the GDPR entered into force and we are only a couple of months away from it starting to apply. There is no doubt that the GDPR is the big Game Changer in the privacy world in the EU and beyond. During the two-year transition period since the GDPR entered into force, regulators, legislators as well as private and public sector organisations have devoted significant time and resources in order to get GDPR-ready. Despite all these efforts, it appears that across the spectrum, the bulk of the work is still to be done.

For instance, out of the 28 Member States, only two (Germany and Austria) have enacted national legislation supplementing the GDPR. 13 Member States have proposed a Bill and the remainder are further behind (as further explored in our GDPR National Legislation Survey[1]).

Privacy regulators (whether local Data Protection Authorities or the European Data Protection Board) are also still busy coming to terms with their redefined roles and responsibilities and getting their own house in order. Many local data protection authorities currently focus on helping businesses understand, and achieve compliance with, the GDPR and are publishing helpful guidance and compliance tools. Although it does not seem like regulators are contemplating making immediate use of their powers to impose huge fines, enforcement actions are to be expected especially when companies cannot demonstrate sound GDPR compliance programs.

The level of "GDPR maturity" amongst private sector organisations varies considerably. While some kicked into action two years ago and have made good progress in bringing their privacy practices in line with GDPR requirements, others are only starting to wake up to this. Companies should see the GDPR as an opportunity to rethink their approach to data, rather than viewing it merely as a burdensome and costly compliance obligation. It is no secret that businesses that want to become or remain competitive and profitable in the digital age will need to leverage digital solutions, which ultimately live off data. Businesses of all sizes should come up with a smart and compliant data strategy. Such a strategy would combine the two tasks of (1) finding ways to leverage and derive value from data, and (2) doing so in a privacy-compliant way. While such a strategy will need to take into account local data protection laws and requirements, the GDPR would be the best starting point for a comprehensive global privacy program.

To assist organisations with this process, we at Baker McKenzie have devised a GDPR Game Plan and are pleased to present the 2018 edition. We have identified 13 areas of particular interest (the so-called 'Game Changers') that organisations need to be aware of and address as a matter of priority. In this publication, we explain each of those Game Changers in detail and offer practical steps for addressing the new requirements. At the start of the publication, you will also find a brief overview of the 13 Game Changers.

We trust that you will find this publication helpful. A special thanks to our various privacy practitioners for their contributions to this publication. Please do not hesitate to get in touch with any of our privacy practitioners with any questions, comments or other feedback. We would be delighted to hear from you!

Elisabeth Dehareng
Partner, Brussels
elisabeth.dehareng@bakermckenzie.com

Francesca Gaudino
Partner, Milan
francesca.gaudino@bakermckenzie.com

Anna von Dietze
Senior Professional Support Lawyer, Dusseldorf
Anna.vonDietze@bakermckenzie.com

[1] The survey is available at tmt.bakermckenzie.com

Contributors

Magalie Dansac Le Clerc
Partner, Paris
+33 1 44 17 59 82
magalie.dansacleclerc@bakermckenzie.com

Elisabeth Dehareng
Partner, Brussels
+32 2 639 36 11
elisabeth.dehareng@bakermckenzie.com

Anna von Dietze
Senior Professional Support Lawyer, Dusseldorf
+49 211 3 11 16 300
anna.vondietze@bakermckenzie.com

Daniel Fesler
Partner, Brussels
+32 2 639 36 58
daniel.fesler@bakermckenzie.com

Francesca Gaudino
Partner, Milan
+39 02 76231 452
francesca.gaudino@bakermckenzie.com

Julia Kaufmann
Partner, Munich
+49 89 5 52 38 242
julia.kaufmann@bakermckenzie.com

Magdalena Kogut-Czarkowska
Associate, Warsaw
+48 22 4453452
magdalena.kogut-czarkowska@bakermckenzie.com

Yann Padova
Partner, Paris
+33 1 44 17 59 27
yann.padova@bakermckenzie.com

Noëlle Pineux
Associate, Brussels
+32 2 639 37 29
noelle.pineux@bakermckenzie.com

Raul Rubio
Partner, Madrid
+34 91 230 45 35
raul.rubio@bakermckenzie.com

Michael Schmidl
Partner, Munich
+49 89 5 52 38 211
michael.schmidl@bakermckenzie.com

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

Michaela Weigl
Associate, Frankfurt
+49 69 2 99 08 368
michaela.weigl@bakermckenzie.com

Baker McKenzie's GDPR Game Plan

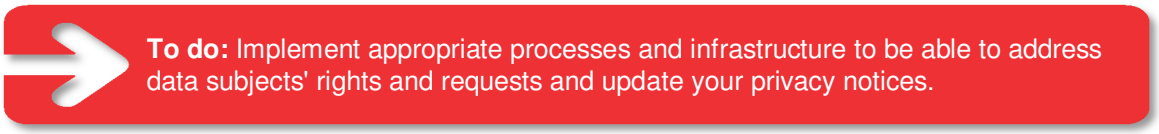
EU General Data Protection Regulation in 13 Game Changers

What businesses need to know and do to prepare

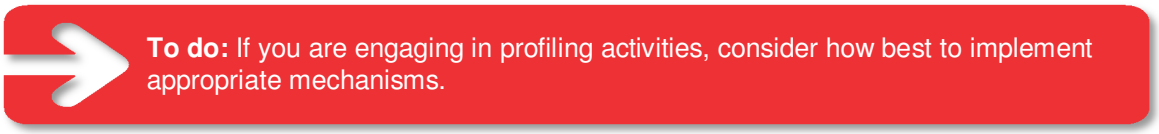
As of 25 May 2018, the EU General Data Protection Regulation ("**GDPR**") replaces the Data Protection Directive 95/46/EC (**"Directive"**) and is directly applicable in all EU Member States without need for implementing national laws. Here are our 13 Game Changers which businesses should address as a priority in order to make their data protection compliance programs, processes and infrastructure fit for GDPR.

1. **Expanded Scope and One-Stop-Shop under the GDPR:** 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). [pp 7-11]

2. **Data Subjects' Rights under the GDPR:** 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. [pp 12-16]



3. **Profiling and Profiling-Based Decision-Making under the GDPR:** 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. [pp 17-20]



4. **Consent under the GDPR:** 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. [pp 21-27]

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 Processor Obligations under the GDPR:** 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. [pp 28-32]

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 under the GDPR and Beyond:** Controllers and processors will have to maintain record of processing activities. Detailed information must be kept and provided to supervisory authorities upon request. In addition, data mapping is an essential first step in establishing a privacy compliance program and should be seen as an audit of an organisation's assets. [pp 33-36]

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 Requirements under the GDPR:** 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. [pp 37-40]

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 Assessment under the GDPR:** Controllers will be required to perform a Data Protection Impact Assessment (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 the 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. [pp 41-44]

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 Obligations under the GDPR:** 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. [pp 45-48]

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. **EU Data Protection Officer - Must Have, Nice to Have or Safe to Ignore?** 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. [pp 49-54]

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. **Cross-Border Data Transfer Rules under the GDPR:** 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. [pp 55-58]

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. **New Pan-European Data Breach Notification Obligations:** 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. [pp 59-62]

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 and Sanctions under the GDPR:** 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). [pp 63-69]

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.

Game Changer 1: One-Stop Shop under the GDPR

The one-stop-shop ("**OSS**") mechanism incorporated into the GDPR was probably the most controversially discussed concept during the GDPR's inception. What we are left with, is a considerably watered-down version of the EU Commission's ambitious initial proposal for streamlining the competencies of the various national supervisory authorities ("**SAs**") and ensuring a consistent interpretation and application of the GDPR by them.

1. Key Takeaways

(a) As a **general rule**, each SA will be competent to perform the tasks assigned to it and exercise the powers conferred on it on the territory of its Member State. Without any qualifications or derogations, this rule would frequently lead to various national SAs being competent to act on one and the same matter.

(b) In order to promote consistency and ease the compliance burden for businesses, **in cases of "cross-border processing", generally only the SA of the main or single establishment of the controller/ processor will be competent to act as "lead SA"**, subject to an obligation to cooperate with other "concerned SAs". The idea is that businesses operating in multiple EU locations will have to deal with only one lead SA (where they have their main or single establishment) which will be responsible for supervising all of its processing activities across Europe.

(c) However, the **OSS mechanism is subject to important derogations**. For example, a local SA other than the lead SA may be competent to handle complaints lodged with it or a possible infringement of the GDPR if the subject matter relates only to an establishment in its Member State or substantially only affects data subjects in its Member State.

(d) The GDPR sets out **detailed rules for lead SAs and concerned SAs to cooperate in cases of cross-border processing**. Overall, the lead SA should closely involve and coordinate the concerned SAs in the decision-making process and decisions are to be agreed jointly with disputes to be resolved by the European Data Protection Board ("**EDPB**").

(e) In order to ensure a **consistent application** of the GDPR across EU Member States, the GDPR requires SAs to obtain the opinion of the EDPB before adopting certain measures (such as Binding Corporate Rules or standard contractual clauses) or issuing certain guidance (e.g., when DPIAs are required). In cases of conflict, the EDPB has the last word and may issue binding opinions.

(f) It remains to be seen how the complex rules will be **interpreted and applied in practice**.

2. SA competencies and the OSS mechanism under the GDPR

Under the GDPR, each Member State will continue to be required to establish one or more independent public authorities responsible for monitoring and enforcing the application of the GDPR (for more information on the powers and tasks of national SAs, please refer to our Enforcement & Sanctions Article in this booklet). Existing SAs are likely to play that role in all Member States.

However, the GDPR contains new rules regarding the competencies and cooperation between such SAs.

(a) The general rule

As a general rule, each SA will be competent to perform the tasks assigned to it and exercise the powers conferred on it on the territory of its Member State (Article 55). According to Recital 122, this should be particularly the case where the processing:

- is carried out in the context of the activities of an establishment of the controller/ processor on its territory;
- is carried out by public authorities of that Member State;
- affects data subjects on its territory; or
- is carried out by a controller/ processor not established in the EU when targeting data subjects on its territory.

(b) Special rules for cross-border processing cases

However, in cases of "cross-border processing", generally only the SA of the main or single establishment of the controller/ processor will be competent to act as "lead SA", subject to an obligation to cooperate with other "concerned SAs" (Article 56(1)).

The term "**cross-border processing**" is defined in Article 4(23). In a nutshell, it comprises:

- data processing by controllers/ processors established in more than one EU Member State which processing takes place in the context of the activities of establishments in more than one Member State; and
- data processing which takes place in the context of the activities of a single establishment of a controller/ processor in the EU but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(c) Derogations

By way of derogation from this rule for cross-border processing, each SA shall be competent to handle a complaint lodged with it or a possible infringement of the GDPR if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State (Article 56(2)). So, there will be room for local SAs to argue that they will be competent in cross-border processing cases even though they would technically not qualify as "lead SA". The final decision as to who will handle the matter in these cases rests with the lead SA (Article 56(3)). Further, the OSS mechanism does not apply in cases of data processing by public authorities or private bodies acting in the public interest (Article 55(2), Recital 128).

(d) Lead SA versus concerned SA

The competent **lead SA** will be the SA of the main establishment or of a single establishment of the controller or processor engaging in the cross-border processing in question.

- The **main establishment of a controller** with establishments in more than one Member State is generally the place of its central administration within the EU. However, if the decisions on the purposes and means of processing are taken in another establishment of the controller in the EU and the latter establishment has the power to have such decisions implemented, then that other establishment is to be considered the main establishment.
- The **main establishment of a processor** with establishments in more than one Member State is also generally the place of its central administration in the EU. If a processor has no such central administration in the EU, its main establishment is its establishment in the EU where the main processing activities in the context of the activities of an establishment of the processor take place to the extent the processor is subject to specific obligations under the GDPR. In cases involving both the controller and processor, the lead SA of the controller will be the lead SA for the processor as well but the SA of the processor's main establishment will then be the "concerned SA" (Recital 36).

When it comes to interpreting the term "establishment", one will still need to refer to the CJEU's interpretation of that term. Whether an establishment is a "main establishment" will be considered on

the basis of the processing operation at hand. In respect of each such processing operation an assessment must be made of where the 'effective and real exercise of management activities' takes place.

A SA will be a "**concerned SA**" in the following cases:

- a relevant controller or processor has an establishment on the territory of its Member State;
- data subjects residing on the territory of its Member State are substantially affected or likely to be substantially affected by a processing in question; or
- a complaint has been lodged with it (regardless whether that complaint has been lodged by a data subject residing in that Member State or elsewhere).

In practice, the designation of lead SAs and concerned SAs as well as their cooperation will be challenging processes. The Article 29 Working Party ("WP29") issued "Guidelines for identifying a controller or processor's lead supervisory authority" (adopted on 13 December 2016 and last revised on 5 April 2017). These Guidelines clarify that:

- The controller or processor is responsible for proving its decision regarding the lead SA. Therefore, a company should be careful in documenting the reasons of its decision to identify the lead SA.
- The SAs concerned and the SA identified as the lead SA by the controller or processor can challenge the controller or processor's decision and ask for additional evidence supporting this decision. The SAs will ultimately determine which SA is the lead SA. No 'forum shopping' is allowed meaning that the company must identify the lead SA in the country of the establishment which has actual and effective decision making power in respect of data processing.
- If a controller has no EU establishment with central administration or decision making power in respect of processing, the one-stop-shop (i.e. the simplified process of having a lead SA) will apply only if the controller designates a main establishment in the EU and this establishment has real and effective decision making power with respect to data processing. This includes taking liability for the processing and the ability to implement its decisions. The mere designation of a representative in a Member State does not trigger the one-stop-shop mechanism.
- Whether a processing operation is considered a "cross-border processing" and results in a lead SA having jurisdiction will not be clear in all events. It depends on a number of factors, such as the context of the processing, the type of data, the purpose of the processing, the impact of the processing on data subject and the number of data subjects involved.
- A controller that is established in multiple EU countries may need to identify more than one lead SA if the controller has different decision making centres in different EU countries, with respect to different processing activities.

Companies can influence the nature of their processing operation to some extent. If they structure the data processing operations in such way that one entity will have control over and responsibility for the means and the purposes of the processing of personal data in several countries, this processing is likely to be considered "cross-border".

However, other SAs may be able to work around the OSS mechanism by focusing their investigation or enforcement activities purely on the activities and effects in their own jurisdiction. Where an SA intends to interfere in "processing operations which substantially affect a significant number of data subjects in several Member States", the OSS mechanism applies.

- Only few SAs have issued detailed guidance on how they intend to interpret and apply the OSS mechanism and how a controller or processor could get more clarity as to whether the SA is likely to accept its position as the lead SA. At the time of publication, the most detailed local

guidance is Guidance Note IR02/17 of the Gibraltar Regulatory Authority[2], published on 24 May 2017. As many organisations have questions on how the OSS works in practice, additional guidance and information at national level is expected.

(e) Rules for cooperation between lead SA and SAs concerned

Article 60 sets out detailed rules for lead SAs and concerned SAs to cooperate in cases of cross-border processing. For example, they shall exchange information, the concerned SA shall provide assistance to the lead SA upon request (e.g., by conducting inspections or investigations), the lead SA shall keep concerned SAs informed on a particular matter and seek their input on draft decisions. Overall, the lead SA should closely involve and coordinate the concerned SAs in the decision-making process. Decisions are to be agreed jointly between the lead SA and concerned SAs following a complex process for sharing draft decisions, taking into account relevant and reasoned objections by concerned SAs in relation to them and adopting mutually agreed decisions. Where SAs have conflicting views as to which SA is competent to act or cannot jointly agree a decision, the matter will be referred to the EDPB for resolution (see below under "Consistency mechanism"). This cooperation requirement is subject to an urgency exception. A concerned SA may immediately adopt provisional measures intended to produce legal effects on its own territory and valid for no more than three months if it has reasons to consider that there is an urgent need to act in order to protect the interests of data subjects (Articles 60(11) and 66). Such urgent need to act may arise, for example, because otherwise the enforcement of a right of a data subject could be considerably impeded (Recital 137). It remains to be seen how this exception will be interpreted.

(f) OSS in data breach notification scenarios

The OSS mechanism is particularly important in data breach notification scenarios where a breach relates to a 'cross-border' processing. If there is sufficient clarity on which Sa is the lead SA, the controller should notify that lead SA and not SAs of other Member States affected by the breach. In that notification it will generally have to disclose in what countries the data breach has or may have an impact, for instance because the data subjects involved are located in different countries across Europe.

If the controller has doubts as to which authority is the lead SA for the relevant processing, it should, at a minimum, notify the local supervisory authority where the breach has taken place (see the Art. 29 Working Party "Guidelines on Personal data breach notification under Regulation 2016/679"). If the controller has not identified its lead SA, it will probably have to notify the SAs in all affected countries.

3. Consistency mechanism

The GDPR contains a much discussed "consistency mechanism" (Articles 63 to 67) intended to ensure a consistent application of the GDPR across the EU (one of the major downfalls of the current regime under the Directive). The EDPB, which will replace the Article 29 Working Party and comprise the European Data Protection Supervisor and the heads of the national SAs, will play an important role in this regard by issuing opinions and guidance, reporting to the EU Commission and resolving disputes between SAs.

One aspect of the consistency mechanism is the above-mentioned referral of disputes between SAs on particular matters to the EDPB for resolution. Further, according to the consistency mechanism, SAs must obtain the EDPB's opinion before they adopt any of the measures listed in Article 64(1), such as Binding Corporate Rules, standard contractual clauses or lists of processing operations that fall under the DPIA requirement. While the GDPR sets out a complex consultation process for consultation between SAs and the EDPB, the EDPB will ultimately retain the last word and be able to issue a binding opinion in case of disagreement.

[2] Guidance Note IR02/17 of the Gibraltar Regulatory Authority

4. Your OSS Game Plan

Businesses operating in more than one EU jurisdiction - either because they are established or because they target individuals in multiple EU jurisdictions will be most affected by the OSS mechanism.

Those businesses should:

- identify their "main establishment" (in case they have several EU establishments) to identify their likely lead SA. In some cases, businesses might be able to influence which SA will be their lead SA by structuring their data processing operations and decision making in a certain way. While forum shopping should be avoided, in some instances small structural changes to operations might be sensible and appropriate;
- document their decision identifying the lead SA. Clear and robust documentation of the reasons underlying the decisions are recommended;
- monitor their lead SA closely for guidance and other output issued and understand their enforcement priorities;
- start to engage and establish good relations with their lead SA. Discussing cross-border data processing operations with the SA identified as lead SA, may be useful to get more clarity on the relevant authority's view on its "lead SA" status;
- identify likely "concerned authorities" that their lead SA might consult with over their processing activities and get to know them; and
- watch out for further guidance on the how the OSS will be interpreted and applied in practice.

* * * * *

Please contact your usual Baker McKenzie contact to help you identify your likely lead SA/ concerned SAs, assess whether it might be advisable to restructure your processing operations in light of the OSS and for other guidance on the OSS and related mechanisms.

Game Changer 2: Data Subjects' Rights under the GDPR

The GDPR dedicates a whole chapter to data subjects' rights which controllers are required to honour. The intention is to strengthen and expand data subjects' rights compared to rights granted to them under the Directive. Infringements of the provisions relating to data subjects' rights are subject to the maximum level of fines under the GDPR. Controllers would therefore be prudent to prioritise compliance with these obligations.

1. Key Takeaways

(a) The GDPR **expands data subjects' rights existing under the Directive** such as the right to access, right to rectification and right to object.

(b) The GDPR **introduces important new rights for data subjects**, namely the right to data portability and certain rights in relation to profiling. In addition the right to erasure, which was already present under the Directive, is extended and re-interpreted so that it may be regarded as a new right, usually referred to as the 'right to be forgotten'.

(c) Under the GDPR, controllers will be required to **provide significantly more information about their processing activities to data subjects**. Complying with the new information requirements will require controllers to update their privacy policies and to translate these requirements into internal policies and procedures in order to be prepared to comply with the new obligations, also in light of the high sanctioning threshold.

(d) Organisations will be able to **have a single EU-wide privacy policy** to the extent their processing operations are the same across the EU and do not fall within the areas that are granted a certain degree of national differentiation under the GDPR - for example, HR or other highly regulated sectors. The policy should be made available in the relevant local languages.

2. Data subjects' rights under the GDPR

The GDPR retains the rights granted to data subjects under the Directive. However, the GDPR partly amends and adds to them and - once again - is more prescriptive than the Directive. Profiling restrictions and data subjects' related rights are covered in a separate article in this booklet.

(a) Information rights

In order to guarantee fair and transparent processing, the GDPR explicitly requires controllers to communicate with data subjects and provide information to them about data processing activities in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Visualisation through standardised icons is encouraged. Extra-care must be taken when addressing children.

Art. 13 of the GDPR contains a long list of information to be disclosed to data subjects at the time that personal data is collected from them. While quite a few of the items listed must already be disclosed to data subjects under the Directive (such as the identity of the controller and the processing purposes), many of these items are more detailed or entirely new. More specifically, under the GDPR, controllers must provide to data subjects information on the following points (which information is not required to be provided under the Directive but might be required to be provided under some Member State laws):

- the contact details of the data protection officer (if any);
- the legal basis for any processing, including legitimate interests pursued by the controller or third party (if applicable);

- very specific details regarding international data transfers, including references to an adequacy decision (if applicable) or to suitable safeguards implemented;
- the period for which personal data will be stored or, if this is not possible, the criteria for determining such period;
- the right to object to data processing in certain cases (such as direct marketing);
- the right to data portability;
- the right to withdraw consent at any time;
- the right to lodge complaints with supervisory authorities;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract;
- whether data subjects are required to provide the data and the possible consequences for failing to provide data; and
- the existence of automated decision making (including profiling) as well as the logic involved and the significance and envisaged consequences of such processing for the data subject.

Like the Directive, the GDPR distinguishes between:

- instances in which data is collected directly from data subjects in which case the above information must be provided at the time of the collection of the data; and
- instances in which data is not obtained from data subjects, in which case the above information (subject to minor changes) must be provided to data subjects at the latest one month after the data was obtained.

The above information provision requirements do not apply in cases where the data subject has the information already, where the provision of information proves impossible or would involve a disproportionate effort, where the data is subject to professional secrecy obligations, or where Union or Member State law requires the obtaining or disclosure of data.

Controllers will be required to review and update their privacy notices and other documents informing data subjects about their data processing practices in order to reflect the new plain language and information provision requirements. In addition, for the case when data is not obtained directly from the data subjects, the GDPR introduces a specific deadline: one month to inform data subjects. Conveying all of the above information to data subjects will likely be challenging in practice at times. Conversely, the operational benefit for controllers is that they will be able to rely on one pan-European privacy notice provided their data processing activities are the same across Europe and do not fall within the areas that are granted a certain degree of national differentiation under the GDPR - for example, HR or other highly regulated sectors. The privacy notices should be translated into relevant local languages. While the GDPR does not expressly require the latter, a privacy notice in foreign language would not satisfy the requirements of transparency and of being easily understandable by data subjects.

(b) Access requests

Data subjects retain their right to request access to their personal data that is being processed by a controller. Both the Directive and the GDPR set out a list of information that controllers must provide in response to such access requests, but the GDPR provides for a richer set of information to be made available to the data subjects upon request.

Other changes introduced by the GDPR include:

- controllers must put in place processes for facilitating the data subject's exercise of their rights, including processes for making requests electronically;
- access requests must be dealt with free of charge subject to an exception for manifestly unfounded or excessive requests;
- controllers must respond to access requests without undue delay, and at the latest within one month, subject to a two-month extension for complex requests or large numbers of requests; and
- controllers should use all reasonable measures to verify the identity of data subjects requesting access before granting access.

(c) Right to rectification

Data subjects also retain their right to rectification under the GDPR which requires controllers, upon request, to rectify inaccurate personal data and complete incomplete personal data. .

(d) Right to object

Under the GDPR, data subjects will have broader rights to object to data processing activities. Specifically, they will be able to object to processing of their personal data based on legitimate interests without having to demonstrate compelling legitimate grounds for such objection (as is required under the Directive). Rather, where the controller wishes to continue to process such data despite an objection, it will be required to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject, or to demonstrate that the processing is necessary for the establishment, exercise or defence of a legal claim.

Data subjects retain their right to object to processing of their personal data for direct marketing purposes (including the right to object to profiling related to direct marketing).

(e) Right to erasure

The GDPR expands the right to erasure that was contained in the Directive (also referred to as the 'right to be forgotten'). Data controllers will be required to erase personal data upon request and without undue delay if one of the following grounds is met:

- the data is no longer necessary for the purpose for which it was collected or otherwise processed;
- the data subject withdraws consent on which processing is being based and no other legal processing ground can be relied on;
- the data subject validly objects to the processing pursuant to Article 21;
- the data has been unlawfully processed;
- the erasure is required for compliance with a legal obligation under Union or Member State law; or
- data has been collected in relation to the offering of information society services to a child.

The circumstances in which personal data must be erased are not all new and partially exist already under national data protection legislation (such as in Germany and Italy). The above also does not codify a broad right to be forgotten as was established by the CJEU in the *Google Spain v Costeja* decision.

Importantly, where controllers have publicised personal data that they are obliged to erase, they are required to take reasonable steps (taking into account available technology and costs) to inform

other controllers who are processing the data, that the data subject has requested the erasure of any links to, or copy or replication of, such data.

The right to erasure is subject to a number of exemptions, including where the data processing is necessary for exercising the right to freedom of expression and information, for compliance with a legal obligation or for the establishment, exercise or defence of legal claims. .

(f) Right to data portability

The GDPR introduces a new right to data portability. Namely, to the extent data subjects have provided their personal data to a controller, and the controller processes that data by automated means and on the basis of consent or a contract, data subjects may require the controller to:

- provide them with their personal data in a structured, commonly used and machine-readable format; and
- where technically feasible, transmit that data directly to another controller.

While controllers are encouraged to develop interoperable formats that enable data portability, they are not required to adopt processing systems that are technically compatible.

Although the right to data portability is limited (e.g., it only applies where a data subject has provided personal data to a controller and the data is processed by automated means and on the basis of consent or in performance of a contract), this right will require many controllers to implement technical processes to honour this right and might well result in a requirement to hand over valuable personal data to a competitor.[3]

(g) Right to restriction of processing

Data subjects also have the right to restrict the processing of personal data in the following instances:

- a data subject contests the accuracy of personal data and the controller is in the process of verifying the accuracy of the data;
- processing is unlawful but the data subject requests the restriction of the processing rather than an erasure of the data;
- the controller no longer needs the personal data for the purposes of processing but the data subject requires the data for the establishment, exercise or defence of legal claim; or
- the data subject has objected to the processing and a decision is pending as to whether the controller may continue to process the data on the basis of legitimate interests.

In case of such a processing restriction, controllers may store the relevant data but may no longer in any other way process it, except with the data subject's consent, for the establishment, exercise or defence of legal claims or for reasons of important public interest. Before processing restrictions are lifted, the controller must inform the data subject accordingly.

3. Game Plan

We recommend the following Game Plan for ensuring compliance with obligations in relation to data subjects' rights.

[3] Guidelines on the right to data portability were issued by the Article 29 Working Party on 13 December 2016 (as of 10 March 2017, these guidelines are under final review by the Article 29 Working Party after having been submitted for public comments)

(a) **External Privacy Notices**. Review and where necessary revise your privacy notices in order to reflect the new information requirements. In particular, these need to be expanded to convey all the additional information required to be provided to data subjects. They might also need to be edited to conform to the new transparency and plain language requirement. Consider a EU-wide privacy policy (subject to translation into local language).

(b) **Internal Privacy Policies**. Revise your internal privacy policies to ensure they reflect your organisation's obligations in relation to data subjects' rights. This will help ensure that your employees are aware of the new requirements but should be complemented by employee training (see below).

(c) **Checklists**. Given the breadth of the new requirements, we recommend creating checklists for internal use to ensure compliance with the various requirements. These could include checklists for handling access requests, checklists as to when data must be erased or rectified and checklists as to what information must be provided to data subjects.

(d) **Systems and procedures**. Consider what system implementations and processes are required to enable your organisation to comply with the various new requirements. For example, you may need to put in place new processes to facilitate the exercise of data subjects' access rights and to ensure prompt and adequate handling of access requests. You may also need to implement systems allowing you to comply with data portability requirements.

(e) **Training**. Support your new policies and procedures by adequate training to ensure relevant employees are aware of the new requirements and know how to respond to requests.

We also recommend that organisations treat compliance with these obligations as a matter of priority given the potentially significant fines for violations of these obligations.

* * * * *

Please contact your usual Baker McKenzie contact for assistance in revising or drafting your privacy policies, notices and checklists and for designing and implementing procedures and processes to ensure compliance with your organisation's obligations vis-à-vis data subjects.

Game Changer 3: Profiling and Profiling-Based Decision-Making under the GDPR

In today's times of big data analytics and personalised customer experiences, businesses of all sizes and sectors increasingly collect large amounts of personal data in order to create detailed profiles of data subjects recording their behaviours, preferences, movements, etc. Further, businesses increasingly make decisions based on those customer profiles (such as granting or refusing loans). In an attempt to control and limit these activities seen as a threat to privacy, the GDPR imposes restrictions on data controllers that engage in these activities.

5. Key Takeaways

(a) **Profiling** is a form of data processing and as such is not prohibited but **subject to the general rules governing the processing of personal data**.

(b) Individuals have certain **rights to object to profiling** which must be honoured by controllers.

(c) Controllers are subject to **specific information requirements** where they engage in profiling.

(d) Individuals have the **right not to be subject to a decision based solely on profiling (or other automated processing activities)** which produces legal effects concerning them or similarly significantly affects them. This right is subject to **limited exceptions**, namely that the decision is:

- based on the data subject's **explicit consent**;
- **necessary for the entering into, or performance of, a contract** between the data subject and the controller; or
- **authorised by EU or Member State law** to which the controller is subject,

provided in each case suitable measures to safeguard the data subject's rights, freedoms and legitimate interests exist.

(e) Data processing undertaken for the purpose of profiling-based decision-making may be subject to the requirement to carry out a **data protection impact assessment**.

(f) Decisions based solely on profiling (or other automated processing) must not be based on **sensitive data** unless the data subject has explicitly consented or the processing is necessary for substantial public interest reasons on the basis of Union or Member State law.

(g) Profiling-based decision-making must not take place in relation to **children**.

(h) Union or **Member State law may impose further restrictions** in relation to decisions based on profiling.

(i) The Art. 29 Working Party/European Data Protection Board ("**EDPB**") will likely issue **guidance in relation to profiling**, and in particular as to when decision-making based solely on profiling will be permitted.

2. Profiling and related requirements

(a) What is "profiling"?

The term "profiling" is defined in the GDPR and captures essentially any automated data processing that involves the use of personal data to evaluate certain personal aspects of an individual. These personal aspects include in particular aspects relating to the individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Common examples would include tracking people's movements through geo-location technology or tracking peoples' web browsing activities through cookies in order to analyse or predict their purchasing behaviour or build consumer profiles. The Article 29 Working Party in its guidance on automated individual decision-making and profiling emphasizes that while profiling is often used to make predictions about individuals, also simply assessing or classifying individuals based on characteristics such as their age, sex, and height could be considered profiling, regardless of any predictive purpose.

(b) Under what circumstances is profiling permitted?

The activity of profiling as such is not prohibited. But as a form of data processing profiling is subject to the general rules governing the processing of personal data. As such, profiling requires a legal ground (e.g., the data subject's consent or legitimate interests) and must comply with data protection principles.

Recital 71 further spells out that in order to ensure fair and transparent processing, and taking into account the specific circumstances and context in which personal data are processed, controllers shall:

- use appropriate mathematical or statistical procedures for the profiling;
- implement technical and organisational measures appropriate to ensure that the risk of errors and inaccuracies is minimised and that, where they occur, these can be corrected; and
- secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons.

(c) Right to object to profiling

While individuals have no universal right to object to profiling, they may object to profiling in certain instances (depending on the purpose or legal basis of the profiling). In particular, individuals have a broad right to object to profiling for direct marketing purposes (Art. 21(2) and (3)). Any such objection is binding on the controller.

Individuals may further object to profiling that is necessary for:

- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- the purposes of the legitimate interests pursued by the controller or by a third party.

But in these instances, controllers may disregard the objection if they can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of data subjects or if they can demonstrate that the processing is necessary for the establishment, exercise or defence of legal claims.

Controllers must explicitly inform data subjects about their right to object to profiling at the time of the first communication with the data subject. Importantly, the right to object must be presented clearly and separately from other information.

3. Decision-making based on profiling - what is permitted and what is not?

While the activity of profiling is generally permitted, individuals have the right not to be subject to a decision based solely on profiling (or other automated processing activities) which produces legal effects concerning them or similarly significantly affects them. This right is very similar to the right not to be subject to automated individual decisions currently enshrined in Art.15 of the GDPR. By way of example, a decision to refuse an online credit application on the basis of an evaluation of a person's economic situation based solely on profiling without any human intervention would infringe this right. The Art. 29 Working Party gives the example that it would not be permitted to automatically disconnect people from mobile phone services if the bill has not been paid on time. In most (but not all) cases, targeted advertising will not be considered to have a significant legal or similar effect on individuals.

(a) Exceptions

The above right of data subjects is subject to the following exceptions which give controllers some limited room to make decisions based solely on profiling:

- the decision is based on the data subject's explicit consent or *necessary* for the entering into, or performance of, a contract between the data subject and the controller, and the controller has implemented suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or

- the decision is expressly authorised by EU or Member State law to which the controller is subject and the law lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

As regards **consent**, this will most likely be the most common ground that controllers will rely on in practice to justify decision-making based on profiling. However, given the requirement for consent to be explicit and given the specific information requirements imposed on controllers when engaging in profiling, controllers will need to be careful to ensure consents obtained are valid. Please see our article on Consent in this booklet.

As regards the **contracts exception**, this might be a safer ground to rely on than consent where available, but it will only be available in cases of a (pre-)contractual relationship between the controller and the affected data subject which necessitates the relevant decision. The Art. 29 Working Party stresses that the necessity should be interpreted narrowly and that the controller must be prepared to demonstrate that a less privacy-intrusive method for achieving the same purpose could not be adopted.

As regards the **authorisation by EU or Member State law**, these will be narrow provisions and only rarely will controllers be able to rely on this exception. As an example, Recital 71 mentions fraud and tax-evasion monitoring and prevention purposes as well as provisions ensuring the security and reliability of services provided by the controller.

(b) Suitable safeguards

Further, in order to rely on the consent or contracts exception, the controller must have implemented **suitable measures to safeguard the data subject's rights, freedoms and legitimate interests**. In order to satisfy this requirement, firstly, controllers need to ensure they appropriately inform data subjects (at the time of data collection) about:

- the existence of automated decision-making, including profiling;

- the significance and envisaged consequences of such processing for data subjects - tangible examples of the type of possible effects should be given; and

- the logic (i.e., the rationale o relevant criteria) involved. This should include simply given information about the rationale behind, or the criteria relied on in reaching the decision.

- Secondly, controllers must provide the following rights to data subjects (as listed in Recital 71):

- right to obtain human intervention, providing that the reviewer has appropriate authority and capability to change the decision;
- right to express their point of view;
- right to obtain an explanation of a decision reached; and
- right to challenge the decision.

4. Your Profiling Game Plan:

Controllers that engage in profiling activities and/ or make decisions based on such profiling activities will need to be careful not to fall foul of the related restrictions imposed by the GDPR. As a matter of priority, they would be well advised to:

(a) firstly, assess in what respect and to what extent they engage in profiling/ profiling-based decision-making and are therefore caught by the incoming rules;

(b) secondly, ensure that to the extent they engage in profiling, they:

(i) can rely on a legitimate ground to justify the profiling;

(ii) implement internal processes to handle objections;

(iii) update their information notices to adequately inform data subjects about their profiling activities and related rights to object; and

(iv) use appropriate mathematical or statistical procedures for the profiling and minimise the risk of inaccuracies;

(c) thirdly, ensure to the extent they engage in profiling-based decision-making, they:

(i) (in the absence of statutory permissions) either obtain valid explicit consents or are able to demonstrate that the decisions are necessary for the entering into, or performance of, a contract between the data subject and the controller;

(ii) have implemented suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, including that they allow data subjects to express their view, require human intervention and challenge decisions reached; and

(iii) undertake data protection impact assessments if required.

* * * * *

Please contact your usual Baker McKenzie contact for help in assessing whether and to what extent your organisation needs to comply with the profiling-related restrictions of the GDPR and to update your privacy notices, consents and internal information policies and processes to reflect the incoming requirements.

Game Changer 4: Consent under the GDPR

The concept of consent has long been enshrined in European data protection legislation and is a core processing condition under the Directive. The GDPR will retain the concept of consent as a processing condition, and the requirements for consent will largely remain unchanged, although certain new conditions will apply.

Nonetheless, organisations would be well advised to assess the validity of any consents they might be obtaining now or in the future given that (i) consents given under the Directive will remain valid under the GDPR if they conform to the GDPR requirements for consents, and (ii) failure to comply with the consent requirements may trigger the maximum applicable administrative fines under the GDPR.

6. Key Takeaways

(a) Consent as a processing condition is **retained in principle**.

(b) The GDPR is **more prescriptive** when it comes to the conditions for consent but the new rules largely transpose into law what was already required by certain supervisory authorities under the current regime.

(c) The key change is that, under the GDPR, consent will require a **clear affirmative** action. Silence, pre-ticked boxes and inactivity will no longer suffice for there to be valid consent.

(d) The GDPR also introduces a requirement for **parental consent** where information society services are offered to children. The GDPR prescribes that, in an online context, the age of consent is 16, unless Member State law provides for a younger age of consent (which must not be below 13). Based on currently available information, Member States have set the following respective ages for consent:

Country	Age	Notes
Austria	14	According to Austrian Data Protection Act[4]
France	15	According to local draft bill supplementing the GDPR
Germany	16	According to German Federal Data Protection Act[5]
Italy	13	According to local draft bill supplementing the GDPR
The Netherlands	16	According to local draft bill supplementing the GDPR
Poland	13	According to local draft bill supplementing the GDPR
Spain	13	According to local draft bill supplementing the GDPR
UK	13	According to local draft bill supplementing the GDPR

(e) **Pre-GDPR consents** will continue to be valid under the GDPR (without any confirmation or other action from data subjects required) provided they conform to the GDPR requirements for consent.

(f) Non-compliance exposes organisations to **substantial fines**.

[4] Available in German at https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdfsig

[5] Available in German at http://www.gesetze-im-internet.de/englisch_bdsg/index.html

2. Consent for all processing activities

Under the GDPR, "consent" of the data subject means any *freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her* (Article 4(11)).

While most of these requirements for consent are not new, the GDPR is much more prescriptive than the Directive when it comes to interpreting these requirements. That said, in most instances, the new clarifications transpose into law what has long been required by supervisory authorities in practice.

On a final introductory note, the GDPR expressly states that to the extent controllers rely on consents obtained under the Directive to legitimise their processing activities, these consents do not need to be obtained again or confirmed by data subjects provided they conform to the GDPR requirements for consents (Recital 171).

(a) Unambiguous

While it is not new that consent must be unambiguous, the GDPR now contains an express clarification that consent requires either a statement or clear affirmative action in order to be valid. The Recitals clarify that such clear affirmative action could include:

- ticking a box in an online context;
- choosing technical settings for information society services;
- or any other statement or conduct which clearly indicates the data subject's acceptance of the proposed data processing activities.

Silence, pre-ticked boxes and inactivity, on the other hand, will not constitute consent. The Article 29 Working Party, in its (draft) Guidelines on consent under the GDPR adopted on 28 November 2017 ("**WP259**"),[6] also underlines that "*consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service*" (p. 16).

(b) Freely given

Consent must be freely given (as is the case under the Directive). The GDPR now clarifies that consent will not be freely given if:

- the data subject has no genuine and free choice or is unable to refuse or withdraw consent without detriment (Recital 42); According to the Article 29 Working Party, the consent can only be valid provided that "*there is no risk of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs)* if the data subject does not consent"[7]; and/or
- there is a clear imbalance between the data subject and the controller (Recital 43).

Many supervisory authorities or local laws, including the Article 29 Working Party in its Guidelines on consent under the GDPR (WP259)[8], already set forth that consents given in these situations are

[6] Available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849.

[7] Guidelines on consent under the GDPR adopted on 28 November 2017 (WP259), p. 8.

[8] See p. 8: "*An imbalance of power also occurs in the employment context. Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. (…) Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1a)) due to the nature of the relationship between employer and employee".*

void (e.g., consents given in an employment context or to public authorities, except under certain circumstances).

Consent is further highly likely to be not freely given if the performance of a contract (including the provision of a service) is made conditional on the data subject's consent to certain data processing activities which are not necessary for the performance of the contract (Article 7(4) and Recital 43). However, the Article 29 Working Party appears to be of the view that the controller can rebut the presumption of a tied consent by showing that data subjects are able to choose between the service for which they must consent to the use of data for additional purposes and an equivalent service that does not involve consenting to data use for additional purposes (WP259, p. 10).

Recital 43 further clarifies that consent is presumed to not be freely given if separate consents are not allowed for different data processing operations when such separate consents would be appropriate. This suggests that bundled consents will often be invalid.

(c) Specific

Consent must relate to specific processing operations (granularity of consent). Consequently, a general broad consent to unspecified processing operations as they might arise will be invalid. To the extent data processing has multiple purposes, a consent to those processing activities should cover all those purposes (Recital 32). Consents should also cover all processing activities carried out for the same purpose or purposes (Recital 32).

This requirement also entails that data controllers should respect the principle of purpose limitation by determining specific, explicit and legitimate purposes for the intended processing activity (Article 5(1b)). Controllers must also clearly separate the information given to data subjects relating to obtaining consent for data processing activities from information about other matters (Article 29 Working Party, WP259, p. 12).

Concerning the time limit, the original consent will no longer be valid if the processing operations change or evolve considerably and a new consent must then be obtained (Article 29 Working Party, WP259, p. 20).

It is worth noting that the requirement for consents to be specific is a little less strict when it comes to data processing for scientific research, especially when research is not based on sensitive data. Such consents are considered valid as long as they cover certain areas of research (rather than specific purposes). This is tribute to the fact that it is often not possible to fully identify the purposes of data processing for scientific research purposes at the time of data collection (Recital 33). In such cases, the Article 29 Working Party considers that controllers may apply further safeguards such as data minimization, anonymization, data security and/or provision of information on the development of the purpose to data subjects (WP259, p. 28).

(d) Informed

Recital 42 clarifies that for consent to be informed, data subjects should understand the fact that and the extent to which they are consenting and be aware, at least, of the identity of the controller and the purposes of the relevant processing. The Article 29 further stated that for consent to be valid, data subjects must be informed of (i) what (type of) data will be collected and used, (ii) the existence of the right to withdraw consent, (iii) the use of data for decisions based solely on automated processing and, (iv) if applicable, the possible risks of data transfers to third countries in the absence of an adequacy decision and appropriate safeguards. Such information must be provided prior to the processing activity for which consent is needed (WP259, p. 13).

(e) Right to withdraw

Data subjects must be able to withdraw their consent at any time and be informed of their withdrawal right at the time of consenting (Article 7(3)). Withdrawing consent must be as easy as giving it. The Article 29 Working Party gives the following example: where consent is obtained

through a service-specific user interface, the data subject must be able to withdraw such consent via the same interface (WP259, p. 21).

Besides, the Article 29 Working Party insists on the fact that the data subject must be able to exercise this withdrawal right without detriment (i.e. free of charge or without lowering service levels) (WP259, p. 21).

The risk that consents may be withdrawn at any time poses a considerable challenge in practice and makes consent a somewhat "unsafe" option.

(f) Formal requirements

As a general rule, consent may be in writing (including in electronic form) or oral form. Caution should be exercised when relying on oral consents as the onus for demonstrating that consent has been obtained clearly is on the controller. Indeed, the Article 29 Working Party provides that, as long as a data processing activity lasts, the obligation to be a able to demonstrate consent exists. Thereafter, the proof of consent should be kept no longer than strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims (Article 17(3b)) (WP259, p. 21).

Pre-formulated consent declarations should be in an intelligible and easily accessible form using clear and plain language and should not contain unfair terms (Article 7(2), Recital 42). Where consents are included in written declarations which also concern other matters (e.g., terms and conditions of purchase), the consents must be presented in a manner that is clearly distinguishable from the other content of the document. Additional safeguards may be necessary to ensure data subjects are aware that they are providing consent and understand the extent of that consent. This will most likely require many businesses to vet and amend their existing legal documents to ensure embedded consents are somewhat set apart from the remainder of the document.

Electronic requests for consents must be clear, concise and not unnecessarily disruptive to the use of the services for which they are provided (Recital 32).

3. "Explicit" consent for certain processing activities

In addition to complying with the above listed requirements, consent has to be "explicit" where it is relied upon to legitimise the processing of sensitive data (Art. 9(2)(a)), profiling activities (Art. 22(2)(c)) or cross-border data transfers (Art. 49(1)(a)). The GDPR does not specify what "explicit" consent entails. Hence, existing interpretations and guidance from supervisory authorities should be consulted in this regard.

The Article 29 Working Party, in an Opinion of 2011 (Opinion 15/2011 on the definition of consent, WP 187), considered that "*[i]n legal terms "explicit consent" is understood as having the same meaning as express consent. It encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing. Usually, explicit or express consent is given in writing with a hand-written signature. For example, explicit consent will be given when data subjects sign a consent form that clearly outlines why a data controller wishes to collect and further process personal data*."

The Article 29 Working Party, in its Guidelines on consent under the GDPR, considers that the term "explicit" means that the data subjects must give an express statement of consent:

- where appropriate, in a written statement signed by the data subjects;
- in the digital or online context (where a written statement is not appropriate), by filling in an electronic form, by sending an e-mail, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature (WP259, p. 18-19).

The Article 29 Working Party does not exclude the use of oral statements but outlines that "*it may be difficult for the controller to prove that all conditions for valid explicit consent were met when the statement was recorded*" (WP259, p. 19).

4. Consent and children

Recognising that children deserve specific protection of their personal data, the GDPR (unlike the Directive) makes express provision for consents provided by children (Art. 8). Essentially, it prescribes that, in an online context, the age of consent is 16 unless Member State law provides for a younger age of consent (which must not be below 13).

More specifically, the GDPR provides that where "information society services" are offered to children, the processing of personal data of a child below the applicable age of consent, requires consent to be given or authorised by the holder of parental responsibility. "Information society services" are defined as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services, and would thus include any chargeable online service offerings. The European Court of Justice, in its judgement of 2 December 2010 in case C-108/09 (*Ker-Optika*), interpreted this notion as contracts and other services that are concluded or transmitted online.

The controller will be required to make reasonable efforts (taking into account available technology) to verify the parental consent. Codes of conduct specifying how parental consents may be obtained might be forthcoming.

The common ceiling of 16 years as the age of consent has sparked outrage at various levels and it would not be surprising to see numerous Member States opt for a lower age of consent. Please refer to our table above on the (draft) data protection laws adopted to date by Member States in that respect.

Lastly, please note that the Article 29 Working Party has extensively examined the issue of data protection of children in relation to information society services, including the interpretation of the conditions of application of Article 8 of the GDPR (e.g., information society service, offered directly to a child, etc.) in its Guidelines WP259 on consent under the GDPR (see p. 23 to 27).

5. Possible Member State divergences

The GDPR provisions on consent allow for a few Member State divergences which organisations need to be aware of. Namely, Member States may opt to adopt:

- an age below 16 as the age of consent (with 13 being the minimum age of consent) ; please see above for an overview of such national divergences (to date);
- rules providing that the prohibition on processing of sensitive data may not be lifted by way of a data subject's consent; and
- specific rules for obtaining consents in an employment context.

6. Guidance of the Article 29 Working Party

As mentioned above, on 28 November 2017, the Article 29 Working Party adopted draft Guidelines (WP259) on consent under the GDPR, thereby completing its existing Opinion 15/2011 on the definition of consent (WP187)[9]. These new draft Guidelines were open for public consultation and are now being finalized.

[9] This Opinion remains relevant as far as it is consistent with the new legal framework. The Opinion 15/2011 is available at http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf.

The Article 29 Working Party provides an in-depth analysis of the notion of consent and the requirements for obtaining and demonstrating valid consent. The Article 29 Working Party starts by explaining the elements of valid consent, i.e. any (i) freely given, (ii) specific, (iii) informed and (iv) unambiguous indication of wishes of data subjects and then further explains what extra efforts are required to obtain the *explicit* consent of data subjects, e.g., for the processing of special categories of data (see references to WP259 in Sections 2 and 3 above).

Furthermore, the Article 29 Working Party provides guidance to controllers on the requirement to be able to demonstrate consent (e.g., see WP259, p. 20: "*the controller may keep a record of consent statements received, so he can show how consent was obtained, when consent was obtained and the information provided to the data subject*") and on the right to withdraw consent (see references to WP259 in Section 2(e) above).

The Article 29 Working Party also addresses the interaction between consent and other lawful processing grounds in Article 6 of the GDPR. It is worth noting that the Article 29 Working Party considers that "*as a general rule, a processing activity for one specific purpose cannot be based on multiple lawful bases. Nonetheless, it is possible to rely on more than one lawful basis to legitimise processing if the data is used for several purposes, as each purpose must be connected to a lawful basis. However, the controller must have identified these purposes and their appropriate lawful bases in advance*" (WP259, p. 22).

Lastly, the Article 29 Working Party focuses on what happens to consent obtained under the Directive and notably states that "*controllers that currently process data on the basis of consent in compliance with national data protection law are not automatically required to completely refresh all existing consent relations with data subjects in preparation for the GDPR. Consent which has been obtained to date continues to be valid in so far as it is in line with the conditions laid down in the GDPR*" (WP259, p. 29).

7. Your Consent Game Plan

While the changes in relation to consent introduced by the GDPR are limited in scope, now is a good time for organisations to check whether their current processes for obtaining consents will meet the GDPR requirements or will require amendments. We recommend that organisations take the following steps:

1. Identify all their processing activities which are legitimised through data subjects' consents.
2. Consider whether it makes sense to rely on consents in all those scenarios or whether other (potentially safer) processing conditions or legal justifications can be relied on in certain instances.
3. Where consent is relied on:
   - **(a)** check that it will be:
     - (i) freely given;
     - (ii) specific;
     - (iii) informed;
     - (iv) unambiguous; and
     - (v) explicit (if required as described above); and
   - **(b)** vet and amend existing (stand alone and embedded) consent forms to ensure they are in line with formal requirements.
4. Ensure processes are in place to promptly honour any withdrawals of consent (including that affected processing operations are stopped).

5. Put in place systems creating reliable records of consents which will enable organisations to demonstrate compliance with consent requirements.

* * * * *

Please contact your usual Baker McKenzie contact for assistance in assessing your existing consents for GDPR compliance, creating GDPR compliant consent forms and processes, creating a consent checklist tailored to your organisation's needs or for any other support you may wish in relation to use of consent for data processing activities.

Game Changer 5: Data Processor Obligations under the GDPR

A major Game Changer under the GDPR will be the new compliance obligations directly imposed on data processors. Given the new liability regime as well as stringent requirements for processing agreements, these changes will have a notable operational impact on many businesses. Controllers and processors alike will need to understand and address the new requirements..

1. Key Takeaways

(a) The **definitions** of "data controller" and "data processor" remain unchanged.

(b) The GDPR will **impose privacy compliance obligations directly on data processors** and **hold them directly liable** for non-compliance with those obligations.

(c) For instance, **data processors will be required** by law to:

- implement appropriate technical and organisational measures to ensure a certain level of data security;
- keep detailed records of their processing activities;
- appoint a data protection officer ("DPO") in certain instances and a representative located within the EU if the processor is located outside of the EU;
- comply with the same cross-border transfer requirements as data controllers; and
- notify data controllers of data breaches.

(d) In the event of non-compliance with their obligations under the GDPR, **processors may be subject to direct enforcement action** by supervisory authorities ("SAs").

(e) The GDPR will not only apply to processors established within the EU or to data processing activities taking place in the EU. The new processor obligations will equally apply to **processors not established in the EU** to the extent the relevant processing activities relate to the offering of goods or services to individuals residing in the EU or to the monitoring of their behaviour.

(f) Controllers and processors will be required to enter into **detailed processing agreements**, the terms of which are prescribed in detail in the GDPR. Most existing processor agreements are unlikely to satisfy the new requirements and will require revision.

(g) **Sub-processors** may only be engaged with the prior consent of the controller and must be subject to the same contractual obligations as the initial processor.

(h) If a **processor acts outside the scope of its authority** granted by the controller, in respect of the relevant processing it will be regarded as a controller and be subject to the same obligations as controllers under the GDPR.

2. The obligations imposed on data processors

The GDPR imposes various privacy compliance obligations directly on data processors:

(a) Security

Processors will be subject to the same data security requirements as controllers. According to Article 32 of the GDPR, they will be required to implement appropriate technical and organisational measures to ensure a level of data security proportional to the risks inherent in the data processing for the rights and freedoms of individuals. Complying with this obligation will require a detailed assessment of various factors including the purposes of data processing activities, potential risks (such as accidental and unlawful destruction or unauthorised disclosure of, or access to, data), the state of the art of security and implementation costs

(b) Record-keeping

Subject to an exemption for small organisations, processors are required to maintain a record of all categories of data processing activities carried out on behalf of a controller (Article 30). Such records must contain, amongst others:

- details of the processor and any controllers on behalf of which the processor is acting as well as their respective representatives and DPOs (if any);
- the categories of processing carried out on behalf of each controller;
- details in respect of international data transfers (if applicable); and
- where possible, a general description of the technical and security measures implemented according to Article 32.

Upon request, processors must make these records available to SAs.

(c) DPO

Processors will be required to appoint a DPO in the same way as controllers will be required to do so (Article 37), namely:

- if their core activities consist of:
  - processing operations which, by virtue of their nature, scope and/or purposes require regular and systematic monitoring of data subjects on a large scale; or
  - processing on a large scale of special categories of data and data relating to criminal convictions and offences; or
- if required by Member State law.

For more information on the DPO requirement, see the DPO article in this booklet.

Furthermore, processors that are located outside of the EU will in general be required to appoint a representative within the EU (Article 27), unless an exception applies.

(d) Cross-border transfer requirements

Processors will be subject to the same cross-border data transfer requirements as controllers. Please see the article on Cross-border Data Transfer Requirements under the GDPR in this booklet.

(e) Data breach notification

While processors will not be required (like controllers) to notify personal data breaches to the SAs or affected individuals, if they become aware of a data breach they must notify such breach to the controller without undue delay to enable the controller to discharge its notification obligations. Even though the term "undue delay" has not been specified by the GDPR, it is likely that a timeframe of 72 hours will be expected by the SAs.

(f) Other obligations

Processors will be subject to a range of additional obligations, including that they will be required to:

- cooperate, on request, with SAs in the performance of their tasks; and
- engage sub-processors only with prior consent of the data controller.

3. Enforcement against data processors

Not surprisingly, under the GDPR SAs will have direct enforcement powers against processors to the extent processors fail to comply with their obligations under the GDPR. SAs may, for example, in the execution of their investigative powers, order processors to provide information or access to personal data or premises. But they may also exercise their corrective powers and issue warnings or reprimands or require processors to bring data processing obligations into compliance with the GDPR. Last but not least, SAs may issue significant administrative fines of up to EUR 20 million against processors, or in case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year (whichever is higher). Please see our Enforcement & Sanctions article in this booklet for a detailed analysis of the enforcement and sanctions regime under the GDPR.

4. Appointing a data processor

The GDPR, in comparison to the Directive, is highly prescriptive when it comes to appointing a processor.

(a) Choice of processor

Controllers must only use processors which provide sufficient guarantees (in particular, in terms of expert knowledge, reliability and resources) to implement appropriate technical and organisational measures as required by Article 32. As it will be difficult in practice for the controller to demonstrate such due diligence, processors' adherence to an approved code of conduct (Article 40) or a certification (Article 42) can serve as sufficient guarantees for appropriate security measures taken by a processor. It is therefore likely that processors adhering to such approved codes of conduct or certifications will have a tremendous advantage over other processors in the market.

(b) Processing agreement

The GDPR requires the controller and processor to enter into a written (including electronic) contract that contains certain prescribed stipulations.

- Firstly, the processor agreement must set out:
- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subjects; and
- the obligations and rights of the controller.

But more importantly the processor agreement must expressly require the processor to:

- process personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing the data, unless that law prohibits such information on important grounds of public interest;
- ensure that persons authorised to process personal data are subject to appropriate confidentiality obligations;
- take all applicable security measures;
- obtain the controller's consent prior to engaging a sub-processor and contractually pass on to the sub-processor the processor's data protection obligations from the processing agreement;

- assist the controller as far as possible in responding to requests by data subjects;
- assist the controller in complying with its obligations relating to data security, data breach notification, data protection impact assessments and related consultation procedures;
- at the choice of the controller, delete or return to the controller all personal data after the end of the provision of data processing services, and delete existing copies unless required by law to retain them; and
- make available to the controller all information necessary to demonstrate its compliance with the requirements for engaging a processor and allow for, or contribute to, audits (including inspections) conducted by or on behalf of the controller.

Importantly, if a processor acts outside the scope of its authority granted by the controller, in respect of the relevant processing it will be regarded as a controller and be subject to the same obligations as controllers. The European Commission or SAs (with the approval of the Commission) may propose data processing agreements that fulfil the abovementioned stipulations.

(c) Sub-processors

The GDPR imposes strict sub-contracting conditions.

- **Consent** - Prior to engaging a sub-contractor in respect of specific processing activities, processors are required to obtain the specific or general written consent of the relevant controller. In the event that only a general consent has been obtained, each time the processor intends to add or change sub-contractors, it should inform the relevant controller and provide an opportunity to object.
- **Contractual requirements** - In any sub-processing contract, the initial processor must pass on to the sub-processor the data protection obligations imposed on the initial processor by the controller.
- **Liability** - If a sub-contractor fails to fulfil its data protection obligations, the initial processor remains fully liable to the controller for the performance of the other processor's obligations.

(d) Liability of data processors (and data controllers)

Data controllers involved in processing are liable for any damage caused by the processing which is not compliant with the GDPR.

Data processors, by way of comparison, are liable for damage caused by processing only if they:

- failed to comply with obligations under the GDPR specifically directed to processors; or
- acted outside or contrary to lawful instructions of the controller.

While the data processor's liability might seem rather narrow compared to the controller liability, this new liability of data processors is significant given that under the Directive processors were not liable for damage caused by processing directly vis-à-vis the data subjects.

Both data controllers and processors are exempt from liability if they can prove that they are not in any way responsible for the event given rise to the damage.

Importantly, in an attempt to ensure effective compensation of data subjects, the GDPR stipulates that controllers and processors involved in the same processing will be jointly liable for the entire damage caused by such processing. While the controller/ processor that pays full compensation under this regime is entitled to claim back part of the compensation from jointly liable controllers/ processors (corresponding to their responsibility for the damage), the risk of being required to fully

compensate data subjects is real, and recourse proceedings against other controllers/ processors may be lengthy and difficult.

5. Game Plan

The new obligations for data processors and data processing agreements will have significant operational impact on both data controllers and processors and will need to be addressed. Here are our respective Game Plans for controllers and processors.

(a) Controller Game Plan

First and foremost, as a controller you will need to:

1. **Reconsider your processor selection process** to ensure you only engage processors that will be able to undertake processing operations in compliance with the GDPR. This may require a more thorough initial vendor due diligence and increased audit rights. But the most effective solution might be selecting only those processors that adhere to approved codes of conduct or have obtained certifications.

2. **Review and assess existing (standard and tailored) processing agreements for GDPR compliance and, most likely, renegotiate and adapt them to make them GDPR compliant**.

(b) Processor Game Plan

Considerable work lies ahead for processors to undertake the following steps (starting sooner rather than later):

6. **Assess whether or not you will fall within the scope of the GDPR**, either because you have an establishment in the EU or the controller is subject to the GDPR.

7. **Understand the new compliance obligations, decide how to comply with them and assess their operational impact**. For example, how will you be discharging your security obligations? What tools/ resources will you put in place to satisfy the record keeping requirements? Do you need to or should you appoint a DPO? Do you need to appoint a representative in the EU?

8. **Identify new responsibilities and risks and consider how to address those**. For example, you will face the risk of direct enforcement action against you which will require resources and will have a financial impact. Those risks will likely need to be reflected in your pricing. You should also carefully consider any risk allocation in your processor agreements.

9. **Understand the market, in particular what data controllers will require from processors moving forward and what your competitors will be willing/ not willing to agree to vis-à-vis data controllers**. One way to do this might be to approach data controllers to get their views on what they will require from processors moving forward (e.g., certifications). This will put you in a position to understand the requirements your clients will expect from you in light of the GDPR.

2. **Devise a strategy for negotiating processing agreements**. Know the requirements, define your negotiables/ non-negotiables and draft your standard processor agreement(s).

* * * * *

Please contact your usual Baker McKenzie contact for assistance in understanding the new data processor requirements, reviewing and/ or drafting standard or tailored processor agreements, devising a sound vendor selection strategy or addressing any other questions or concerns which you may have.

Game Changer 6: Data Mapping under the GDPR and Beyond

In the past years, we have witnessed an exponential increase in the amounts of data that organisations in varying sizes and industries collect and process. Personal data has been heralded as "the new gold" and using personal data smartly will most certainly boost business profitability.

However, using data smartly is easier said than done. A strategic approach which takes into account the operational needs, capacities and goals of an organisation on the one hand and the applicable legal and regulatory privacy requirements on the other hand is required. In particular, compliance with Article 30 (Records of Processing Activities) of the GDPR is crucial. This requires organisations to understand and document (in written or electronic form) the data processing activities they perform, ie, for each data processing activity it is necessary to detail what categories of data are held and processed, for what purposes, who "owns" the data, where does it sit, who gets access to it, for how long data is retained, and to which recipients are data disclosed. It is therefore critical for organisations to understand the data existing in structured but also unstructured form within its estate. This often requires the use of a blend of technologies as well as specialist skills to analyse data output. As a rule of thumb, controllers should be able to identify the 5 Ws (Who/Where/What/When/Why) of personal data under their control at any given time. However, in reality, organisations are often not (or, at least, not sufficiently) aware of exactly what data they collect and for what purposes, who has access to that data, where that data is being held and for how long. This is where Data Mapping comes into play.

7. Key Takeaways

(a) Data Mapping is an **essential prerequisite for any privacy compliance strategy**.

(b) **Data Mapping will help organisations comply** with various GDPR obligations and/ or other applicable privacy laws and regulations.

(c) A Data Map can be a **valuable business asset** beyond privacy compliance as it can deliver various operational benefits, such as improved efficiencies of business processes and IT systems and smarter use of data.

(d) Data Mapping requires a **structured and planned approach** involving various steps and, ideally, the use of specialised software and experts (both legal and technical) to analyse data output.

2. What is Data Mapping?

Data Mapping is the process of identifying, understanding and mapping out the data use and flows of an organisation. A good Data Map will provide a comprehensive overview of the types of data held in an organisation as well as the data flows within, to and from an organisation.

For example, a Data Map will incorporate:

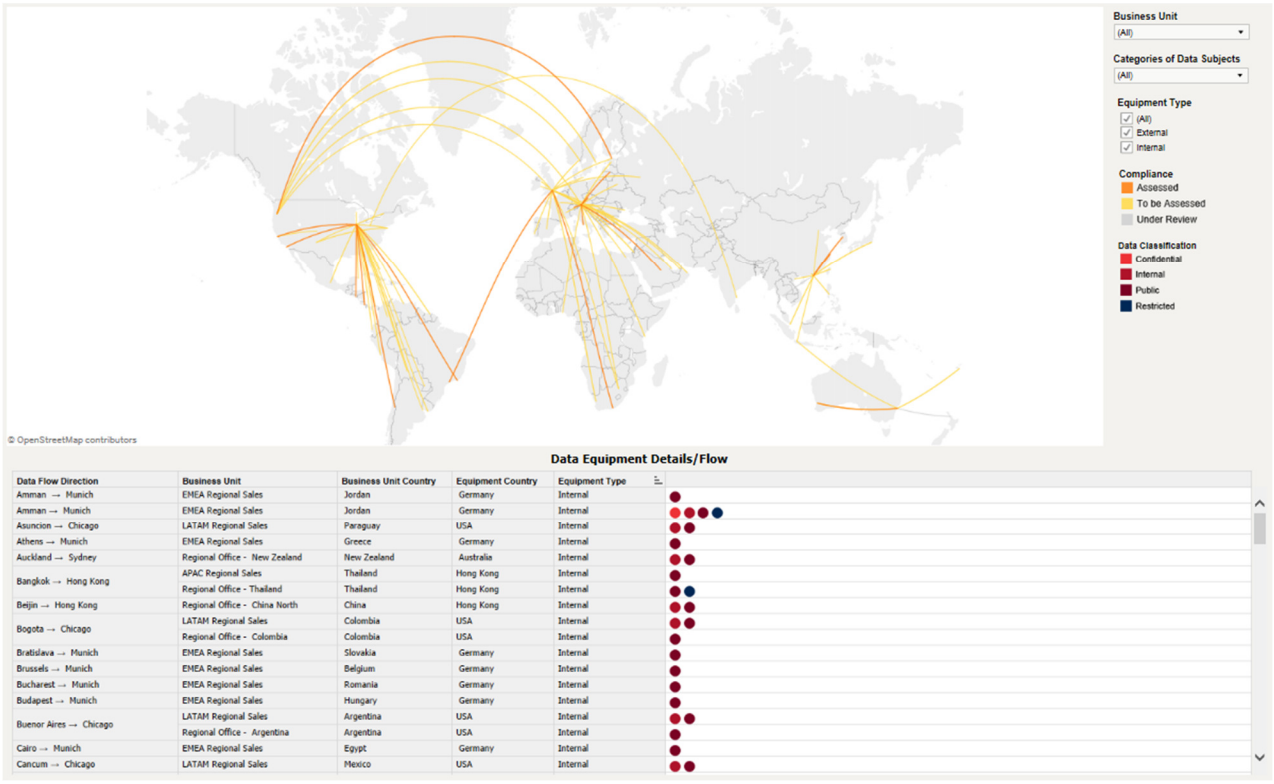
- the various categories of data held and processed by individuals within the business
- the purposes and legal grounds for such processing
- the systems in which the data sits
- the form in which the data exists (eg, structured or unstructured)
- data transfers and disclosures between different business units and to third parties, such as service providers.

In general, Data Mapping requires comprehensive information gathering from all business units globally. The information gathering process should not be a stagnant exercise; rather, it should be a dynamic

consultation with the objective of gaining a comprehensive understanding of various business functions and activities in order to produce a meaningful and truthful Data Map.

3. What does a Data Map look like?

A Data Map can take many forms from a simple spreadsheet to a more complex automated map capturing both structured and unstructured data systems:



Data Flow Direction	Business Unit	Business Unit Country	Equipment Country	Equipment Type
Amman → Munich	EMEA Regional Sales	Jordan	Germany	Internal
Amman → Munich	EMEA Regional Sales	Jordan	Germany	Internal
Asuncion → Chicago	LATAM Regional Sales	Paraguay	USA	Internal
Athens → Munich	EMEA Regional Sales	Greece	Germany	Internal
Auckland → Sydney	Regional Office - New Zealand	New Zealand	Australia	Internal
Bangkok → Hong Kong	APAC Regional Sales	Thailand	Hong Kong	Internal
	Regional Office - Thailand	Thailand	Hong Kong	Internal
Beijin → Hong Kong	Regional Office - China North	China	Hong Kong	Internal
Bogota → Chicago	LATAM Regional Sales	Colombia	USA	Internal
	Regional Office - Colombia	Colombia	USA	Internal
Bratislava → Munich	EMEA Regional Sales	Slovakia	Germany	Internal
Brussels → Munich	EMEA Regional Sales	Belgium	Germany	Internal
Bucharest → Munich	EMEA Regional Sales	Romania	Germany	Internal
Budapest → Munich	EMEA Regional Sales	Hungary	Germany	Internal
Buenor Aires → Chicago	LATAM Regional Sales	Argentina	USA	Internal
	Regional Office - Argentina	Argentina	USA	Internal
Cairo → Munich	EMEA Regional Sales	Egypt	Germany	Internal
Cancum → Chicago	LATAM Regional Sales	Mexico	USA	Internal

Some data protection authorities (for example in Belgium and France) have provided a template that can be used for the Data Mapping (template record of processing activities in Excel format).

4. Why is Data Mapping essential from a privacy compliance perspective?

Understanding one's data features, data flows, data usage, data retention, access and compliance gaps is an essential prerequisite for any privacy compliance strategy. Without understanding what data an organisation collects and processes, why the organisation collects it and where that data flows to and from, it is impossible to ensure that data processing activities become compliant with applicable privacy laws and regulations.

For example, it would not be possible to ensure compliance with cross-border data transfer rules without knowing which types of data an organisation discloses to which recipients and in which countries. Or, how can an organisation adequately secure data if it does not have a complete picture of what data it holds and who has access to it?

From a GDPR perspective, Data Mapping will assist controllers (and, in some instances, processors) to become compliant with various new privacy requirements as they apply to them, including:

- the requirement to maintain detailed records of an organisation's data processing activities and to make these records available to supervisory authorities on request;
- the accountability requirement according to which controllers must ensure and be able to demonstrate that their processing activities are performed in compliance with the GDPR; and

- the data protection by design and by default requirements.

Data Mapping will also assist organisations in assessing the risks of their data processing activities against the rights and freedoms of individuals. Given the risk-based approach advocated by the GDPR, Data Mapping will be an important tool in assessing the extent of applicability of GDPR obligations.

5. What are the additional benefits of data mapping?

In addition to ensuring compliance with legal and regulatory requirements, Data Mapping has multiple other operational benefits. Data Mapping can help organisations in the following ways:

- improve the efficiencies of business processes and IT systems (eg, a Data Map might reveal that data systems and data flows can be streamlined)
- use data in smarter ways (eg, a Data Map may reveal that more efficient data sharing within an organisation might be beneficial - subject to suitable privacy controls and limitations)
- mitigate risks of data breaches (and hence reputational and financial loss)
- respond to discovery requests and reduce related costs
- comply with record retention requirements (while staying GDPR compliant)
- provide valuable insights into data to gain a competitive advantage.

6. Your Data Mapping Game Plan

Given the vast amounts of data being collected and processed by organisations these days, creating a comprehensive Data Map can be a daunting task. The best way to tackle this task is to implement a structured and planned approach including the following steps:

(a) **Appointing a person/ team responsible for creating and maintaining the Data Map.** Ideally, this team would comprise individuals from various business units involved in data processing activities. Alternatively, those individuals should at least assist, and report to, the Data Mapping team.

(b) **Defining a Project Plan.** The Data Mapping team should create a Project Plan which outlines the project scope and level of detail as well as the necessary activities, timelines and responsibilities. For example, the team might decide that only an organisation's most significant or high-risk data processing activities are in-scope as a more comprehensive Data Map which also captures less important data flows might be too costly and difficult to create.

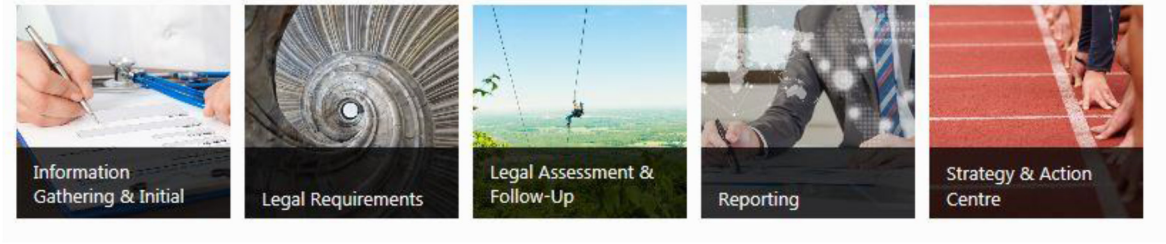
(c) **"Top down" gathering relevant information.** The best way to gather the relevant information will depend on an organisation's business structures and processes in place. But it will most likely require the Data Mapping team to interview and survey individuals involved in the in-scope data processing activities, review IT processes and consult potentially existing (partial) system inventories and other documents.

(d) **"Bottom up" system review - using a blend of technologies.** This process will generally involve a discovery exercise and file analysis, typically over significant volumes of unstructured data.

(e) **Preparing the Gap Analysis Report and Record of Processing based on the information gathered.** At this point, any inefficiencies and gaps in data flows that the Data Maps might reveal should be immediately addressed.

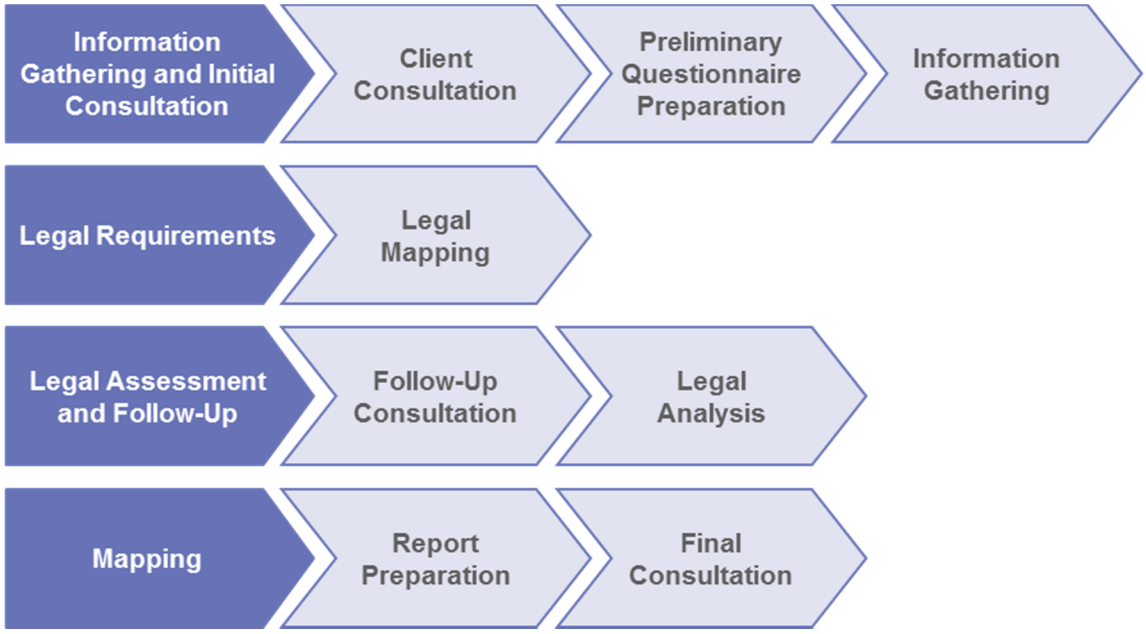
Maintaining and updating the Data Map. Once prepared, the Data Map needs to be regularly updated in order to stay relevant. Ideally, this would be done by automated means as any manual process would be very labour-intensive and would most certainly lead to inaccuracies.

7. Data mapping methodology



iG360, Baker McKenzie's cloud-based end-to-end compliance service, features a special Data Mapping functionality, which assists organisations in creating and maintaining real-time Data Maps. The Data Mapping exercise begins with a thorough information gathering process, followed by an assessment and a comprehensive analysis of the applicable legal requirements using the data gathered. Visualisations in the form of Data Maps are then produced showing all the personal data in an organisation's control and demonstrating all the data flows, usage and access. These Data Maps are intended to help organisations identify the necessary immediate actions in order to safeguard any data flow that may otherwise be inadequately protected.

iG360 Data Mapping Methodology



* * * * *

Please contact your usual Baker McKenzie contact for assistance in creating a Data Map for your organisation or for getting further information on Data Mapping.

Game Changer 7: Data Protection by Design and by Default Requirements under the GDPR

The GDPR expressly codifies the concepts of data protection by design and by default as important data protection principles and imposes specific obligations on controllers in this regard. Compliance with the obligations of data protection by design and by default will form an integral part of any sound data protection compliance program and can also deliver a competitive advantage.

1. Key Takeaways

(a) The new data protection by design and by default requirements **will apply to controllers but not to processors**.

(b) Under the **data protection by design provision**, controllers are required to:

- implement appropriate technical and organisational measures (such as pseudonymisation) which are designed to implement data protection principles (such as data minimisation) in an effective way; and
- integrate necessary safeguards into their processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

(c) What measures will be appropriate in each case will depend on the **risks for rights and freedoms of natural persons** posed by the relevant processing ('risk-based approach').

(d) Under the **data protection by default provision**, controllers are required to implement appropriate technical and organisational measures for ensuring, by default, that only personal data which are necessary for each specific purpose of the processing are processed.

(e) **Obtaining certifications** may help demonstrate compliance with these obligations.

2. Background

While the concepts of data protection by design and by default have been around and discussed for years, they have very rarely been codified in data protection laws around the world until now. They were, however, progressively crafted into recommendations and opinions of the European Commission and of the Article 29 Working Party for specific data protection matters. As for Europe, the concepts are not expressly referred to in the Directive or national data protection laws across the EU. However, they are slowly finding their way into international data protection treaties and national data protection laws and are increasingly being transformed from theoretical data protection principles into legal obligations.

In a nutshell, the concept of data protection by design advances the idea that data protection compliance requires more than mere compliance with legislation and regulatory frameworks. Rather, privacy assurance should become an organisation's default mode of operation, and privacy and data protection must be embedded into the design specifications of technology, business practices and physical infrastructures from the outset as opposed to being added on as a last-minute thought.

The concept of data protection by default is closely related and promotes the notion that, by default, only the personal data necessary for a specific and duly identified purpose must be processed.

3. Data Protection by design under the GDPR

Under the GDPR, controllers are required, both at the time of the determination of the means for processing and at the time of the processing itself, to:

- implement appropriate technical and organisational measures (such as pseudonymisation) which are designed to implement data protection principles (such as data minimisation) in an effective way; and

- integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

Admittedly, these obligations are very vague and hard to translate into tangible requirements. Some guidance can be derived from Recital 78 which provides that appropriate measures to be implemented by controllers could include measures:

- minimising the processing of personal data;

- pseudonymising personal data as soon as possible;

- enhancing transparency about the functions and processing of personal data;

- enabling data subjects to monitor the data processing; and

- enabling the controller to create and improve security features.

Recital 78 further provides that producers of products, services and applications that are either based on the processing of personal data or process personal data to fulfil their task, should be encouraged to take into account the right to data protection when developing and designing such products, services and applications.

However, these are still far from concrete obligations. While it will be challenging to come up with a clear practical plan to comply with the data protection by design obligations, on the positive side this might mean that non-compliance with the obligations will also be hard to attest. So, while there is uncertainty as to the data protection by design requirements, on the positive side, controllers will likely have a degree of flexibility in ensuring compliance with the requirements. This is especially pertinent given that the data protection by design provision incorporates the so-called 'risk-based approach'.

4. Data protection by design and the risk-based approach

The data protection by design provision provides that controllers should implement appropriate measures:

- having regard to the state of the art and the cost of implementation; and

- taking account of the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing (the so-called 'risk-based approach').

In other words, what measures will be appropriate in each case, will depend on the state of the art and the cost of implementation as well as the risks for the rights and freedoms of natural persons resulting from a processing activity. This is very similar to the existing obligations regarding data security under Article 17 of the Directive.

The more likely and severe the risks from the proposed processing, the more measures will be required to counteract those risks. According to Recital 75, processing which could lead to physical, material, or non-material damage would be particularly likely to constitute 'risky' processing requiring particular attention. Recital 75 further provides the following examples as potentially risky processing:

- processing that may give rise to discrimination, identity theft or fraud, financial loss, reputational damage, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;

- processing that might deprive data subjects of their rights and freedoms or prevent them from exercising control over their personal data;
- processing of sensitive personal data or data relating to criminal convictions or offences;
- processing for purposes of profiling;
- processing of personal data of vulnerable natural persons, in particular of children; and
- processing involving a large amount of personal data and affecting a large number of data subjects.

Further guidance on identifying and assessing risks of data processing and on identifying best-practice approaches to mitigate those risks will likely be provided by way of approved codes of conducts, approved certifications and guidelines issued by the European Data Protection Board ("**EDPB**").

Controllers undertaking the types of processing activities listed above or otherwise identified as 'risk' or 'high risk' would be prudent to carefully consider their obligations under the data protection by design provision.

5. Data protection by default under the GDPR

The concept of data protection by default under the GDPR means that the strictest privacy settings should apply by default on data processing. Data controllers must implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of the processing are processed. So, essentially, controllers must aim for data minimisation and structure their systems and processes accordingly. The GDPR further clarifies that controllers must minimise:

- the amount of data they collect;
- the extent of their processing activities;
- storage periods; and
- data accessibility (prescribing that, by default, personal data must not be made accessible to an indefinite number of individuals without the data subject's intervention).

6. Certification mechanisms

The GDPR states that certification mechanisms may be used as an element to demonstrate compliance with the data protection by design and by default requirements. This may be the safest and most suitable way in practice to ensure compliance with these rather vague requirements. It is highly recommended for controllers who regularly participate in public procurement tenders, as the GDPR specifically prescribes that the principles of data protection by design and by default should be taken into consideration in the context of such commercial arrangements.

If nothing else, the certification standards (once set) may provide useful guidance to controllers.

7. Your data protection by design and by default Game Plan

Controllers might want to take the following steps in order to ensure compliance with the incoming data protection by design and by default obligations:

- As an overarching rule, controllers should adopt a proactive approach to data protection rather than simply reacting to complaints, investigations and data protection issues. Controllers should aim to embed data protection into their practices and systems and consider and address data protection requirements and risks at all stages of the information life-cycle (including in the early stages of

developing and designing products, services, applications, etc.). Please refer to our Accountability article in this booklet for further details on taking a proactive approach to data protection.

- Controllers should subject their data processing activities to objective risk assessments, categorise them into 'high-risk', 'medium-risk' or 'low-risk' activities and implement risk-minimising measures accordingly. An important step in this process will be data mapping (see our Data Mapping Article in this booklet).
- Data protection by design requires businesses, at any given time, to identify the "5 Ws" (Who/Where/What/When/Why) of personal data under their control.
- At a more granular level, controllers must always consider the following:
  - minimise the processing of personal data to what is necessary;
  - pseudonymise personal data as soon as possible;
  - be transparent about their data processing activities;
  - prioritise data security and implement appropriate security measures;
  - conduct Data Protection Impact Assessments for high-risk processing activities (please see our article on Data Protection Impact Assessments in this booklet);
  - consider obtaining data protection by design/ by default certifications (especially if they regularly participate in public tenders); and
  - look out for further guidance on the data protection by design and by default principles likely to be issued by regulators, certification bodies, the EDPB and others.

* * * * *

Please contact your usual Baker McKenzie contact for assistance in assessing your current data protection practices against the incoming data protection by design and by default obligations and for ensuring compliance with those obligations.

Game Changer 8: Data Protection Impact Assessment under the GDPR

The GDPR will require controllers to carry out Data Protection Impact Assessments ("**DPIAs**") in cases of potentially high-risk processing activities and to consult supervisory authorities ("**SAs**") in certain instances.

A positive side effect of the introduction of DPIAs will be the abolishment of the general obligation to notify data processing operations to SAs. Rather than generally requiring the notification of data processing operations to SAs (as is currently required in most EU countries), the GDPR will rely on data controllers to assess the impact of envisaged data processing operations and only consult with SAs in relation to high-risk processing operations.

1. Key Takeaways

(a) Where a type of data processing is likely to result in a high risk for the rights and freedoms of individuals, **controllers shall carry out a DPIA prior to the processing** to assess the impact of the envisaged processing operations on the protection of personal data.

(b) The GDPR text itself does not provide much guidance as to what would be considered a "high risk" for the rights and freedoms of individuals. But it does provide a **non-exhaustive list of examples as to when DPIAs will be required and further guidance from SAs can be expected**.

(c) **The GDPR does not prescribe the process for undertaking DPIAs**. Existing or future SA guidance on conducting DPIAs will be the best source of guidance.

(d) If a DPIA carried out by a controller indicates that an envisaged processing would result in a high risk in the absence of risk-mitigating measures taken by the controller, **the controller shall consult the SA prior to the processing**.

(e) The obligations to carry out DPIAs and consult with SAs in relation to high-risk processing operations directly apply to controllers only. But **processors should assist controllers**, where necessary and upon request, in complying with these obligations.

(f) The "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679" from the **Art. 29 Working Party** (WP 248 rev. 01) provide for further guidance regarding DPIAs.

2. DPIAs

(a) What are DPIAs and when must they be undertaken?

A DPIA is an assessment of the impact of envisaged data processing operations on the protection of personal data, and more particularly an assessment of the likelihood and severity of risks for the rights and freedoms of individuals resulting from a processing operation. According to the Art. 29 Working Party, a DPIA is also "a process for building and demonstrating compliance".

Under the GDPR, controllers will be required to undertake DPIAs prior to data processing - in particular processing using new technologies - which is likely to result in a high risk for the rights and freedoms of individuals (Article 35). The GDPR provides the following non-exhaustive list of cases in which DPIAs must be carried out:

- automated processing for purposes of profiling and similar activities intended to evaluate personal aspects of data subjects;
- processing on a large scale of special categories of data or of data relating to criminal convictions and offences;

- systematic monitoring of a publicly accessible area on a large scale.

Recital 91 further indicates that DPIAs will need to be undertaken:

- in case of large-scale processing operations which aim at processing considerable amounts of data and could affect a large number of individuals; or

- as required by SAs which shall publish lists of processing operations which will fall under the DPIA requirement in Article 35(1), such as where data processing operations prevent data subjects from exercising a right or using a service or contract, or because they are carried out systematically on a large scale.

According to the Art. 29 Working Party as a rule of thumb a DPIA would generally be required, if a processing meets two or more of the following criteria (further fleshed out in the guidance): (1) evaluation or scoring, (2) automated-decision making with legal or similar effect, (3) systematic monitoring, (4) sensitive data or data of a highly personal nature, (5) data processed on a large scale, which should be determined based on (a) the number of data subjects concerned, (b) the volume of data and/or the range of different data items being processed, (c) the duration, or permanence of the data processing activity, and (d) the geographical extent of the processing activity, (6) matching or combining of datasets, (7) data concerning vulnerable data subjects, (8) innovative use or applying new technological or organisational solutions, and (9) when the processing itself prevents data subjects from exercising a right or using a service or contract.

The Art. 29 Working Party further recommends that a DPIA is carried out in cases where it is not clear, whether a DPIA is required as a DPIA is a useful tool to help controllers comply with data protection law.

(b) Scope of DPIAs

DPIAs shall contain at least the following information:

- a systematic description of the envisaged processing operations and the purposes of the processing, including where applicable the legitimate interest pursued by the controller;

- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

- an assessment of the risks to the rights and freedoms of data subjects that are likely to result from the processing (and in particular the origin, nature, particularity and severity of such risks); and

- the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and demonstrate compliance with the GDPR.

The GDPR does not prescribe any process or format for DPIAs. For the time being, existing guides on conducting DPIAs issued by local SA will likely be the best source of guidance. The Art. 29 Working Party states that the GDPR provides flexibility when it comes to determining the precise structure and form of the DPIA in order to allow for this to fit with existing working practices. The Art. 29 Working Party expressly outlines that "it is up to the data controller to choose a methodology" (examples are provided in Annex 1 of the guidelines), "but this methodology should be compliant with the criteria provided in Annex 2" of the guidelines.

(c) Existing processing operations

Interestingly, the GDPR is silent on whether the DPIA requirement will apply in relation to processing operations already underway once the two-year transition period finishes and the GDPR provisions start to apply. Strictly speaking, DPIAs must be undertaken before processing operations start which will be impossible in relation to ongoing processing operations. On the one hand, it

seems rather burdensome to expect organisations to assess all of their existing processing operations as to whether they need to be subjected to a DPIA under the GDPR, and then carry out DPIAs, as required. On the other hand, turning a blind eye to existing processing operations and only require DPIAs in relation to processing operations that start following the transition period also does not seem appropriate. The Art. 29 Working Party states in its guidance that the requirement to carry out DPIAs applies to processing operations initiated after 25 May 2018 or to those processing operations that change significantly. Nonetheless, the Art. 29 Working Party strongly recommends to carry out DPIAs for processing operations already under way prior to May 2018. In the absence of further guidance on this point, we would recommend as a best practice approach that organisations identify all of their key, long-term risky processing operations (including ongoing ones) and undertake DPIAs in relation to them.

(d) Other points to note regarding DPIAs

The following other points are noteworthy:

- Where a set of similar processing operations present similar high risks, a single DPIA may be undertaken to address all of those processing operations. In this regard, Recital 92 provides the example of several controllers planning to introduce a common application or processing environment across an industry sector or segment for a widely used horizontal activity.

- Controllers must seek the advice of their DPO (if any) when carrying out DPIAs. According to the Art. 29 Working Party this advice and the decision taken by the controller should be documented within the DPIA.

- Compliance with approved codes of conduct shall be taken into account when assessing the impact of processing operations and may well have a risk-minimising effect.

- Without prejudice to the protection of commercial or public interests or the security of processing obligations, where appropriate, controllers shall seek the views of data subjects (or their representatives) on any intended processing. It remains to be seen in which cases data subjects' views should be sought. According to the Art. 29 Working Party those views could be sought through a variety of means, depending on the context (e.g. a generic study, a question to the staff representatives, or usual surveys sent to the controller's future customers). Furthermore, the reasons for going ahead or not should be documented if the controller's final decision differs from the view of the data subjects, and the controller should document its justification for not seeking the views of the data subjects.

- Controllers shall assess whether their data processing activities are performed in compliance with any applicable DPIA, at least when there is a change of risk represented by the processing operations. Also, according to the Art. 29 Working Party a DPIA should be continuously reviewed and regularly re-assessed. Carrying out a DPIA is a continual process, not a one-time exercise according to the Art. 29 Working Party.

3. Prior consultation procedure

If a DPIA carried out by a controller indicates that an envisaged processing would result in a high risk in the absence of risk-mitigating measures taken by the controller, the controller shall consult the SA prior to the processing (Article 36). Recital 94 seems to slightly soften this requirement by providing that a consultation might not be required if the controller is of the opinion that the identified risk can be mitigated by reasonable means in terms of available technologies and costs of implementation.

If the SA considers that the processing in question would infringe the GDPR, the SA should respond to such requests within eight weeks. However, the eight week period may be extended by six weeks in complex matters and may also be indefinitely suspended until the SA has obtained all information requested for the purposes of a consultation. Consequently, the consultation process may take considerably longer than the projected eight week period. Further, Recital 94 clarifies that a lack of response from an SA within the defined period will not preclude an SA from exercising its powers, such as the power to prohibit processing operations. Hence, a lack of response to a consultation request does

not confirm that an envisaged processing is GDPR-compliant nor does it mean that SAs will not take action against such processing. This might lead to considerable uncertainties in practice.

As part of the prior consultation process, a controller must furnish the following information to the SA:

- where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
- the purposes and means of the intended processing;
- the measures and safeguards provided to protect the rights and freedoms of data subjects;
- the contact details of the DPO (if applicable);
- the data protection impact assessment triggering the prior consultation; and
- any other information requested by the SA.

4. Your DPIA Game Plan

DPIAs will play an important role under the GDPR. The Art. 29 Working Party announced in February that - as a matter of priority - that it will issue (much needed) guidelines or processes on the notion of high risk and DPIAs to help controllers and processors get prepared for the GDPR.[10]

Controllers should take seriously their obligation to carry out DPIAs and we recommend the following steps:

- establish guidelines for what would constitute risky processing operations that will likely require closer scrutiny by way of a DPIA;
- establish policies, processes and templates for carrying out DPIAs and consider how DPIAs can be embedded within the organisation's operational strategy;
- consider what training programmes, threshold analyses and escalation mechanisms are required to allow individuals with access to personal data to be in a position to express their views as to whether a DPIA should be carried out;
- review key (ongoing and planned) data processing operations and identify those that will be subject to the DPIA requirement;
- start carrying out DPIAs as a matter of best practice;
- consider signing up to relevant codes of conduct that might reduce the need for DPIAs; and
- establish processes for consulting with SAs in relation to high-risk processing operations.

* * * * *

Please contact your usual Baker McKenzie contact for assistance in preparing policies, guidelines and templates for carrying out DPIAs, for implementing related processes and for assessing your organisation's processing operations in light of the new requirements.

[10] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf

Game Changer 9: Accountability Obligations under the GDPR

The GDPR expressly introduces a legal accountability obligation to European data protection law. While short in length and inconspicuous on a first reading, the new provisions are likely to have far-reaching consequences in practice.

1. Key Takeaways

(a) Codification of the accountability principle in the GDPR is in line with a **global trend** to make accountability a legal obligation.

(b) Under the **accountability principle as codified in the GDPR**, controllers will be required to implement appropriate technical and organisational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR, and review and update those measures where necessary.

(c) **What measures will be appropriate in each case**, will depend on the nature, scope, context and purposes of the relevant processing as well as the risks for rights and freedoms of individuals.

(d) The GDPR text provides **very little guidance** as to what measures controllers will need to implement to discharge their accountability obligations. Further guidance in the form of codes of conduct, certification mechanisms and clarifications from the Art. 29 Working Party/ European Data Protection Board ("**EDPB**") can be expected.

(e) A **best-practice approach** for organisations to satisfy their accountability obligations would be to build and implement a structured privacy management program. But **less comprehensive approaches** may be appropriate as well, depending on the level of risk raised by the data processing.

2. Background

The notion of accountability is not new to privacy law and policy. It was formally introduced into data protection regulation in 1980 when it was explicitly included as a basic data protection principle in the OECD Guidelines. Since then, the accountability principle has been included in a variety of international data protection instruments as one of several core principles and is slowly (but surely) finding its way into national data protection laws.

While accountability used to be all about allocating responsibility for privacy compliance, it is now about requiring a proactive, systematic and ongoing approach to data protection and privacy compliance through the implementation of appropriate data protection measures - increasingly referred to as "privacy management programs". Various international data protection instruments are being revised to reflect that change.

3. Accountability under the GDPR

Article 24 of the GDPR codifies the accountability obligation. It requires controllers to:

- implement appropriate technical and organisational measures (including introducing data protection by design and by default principles where relevant) to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR; and
- review and update those measures where necessary through notably internal and external assessment such as privacy seals.

Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

(a) What does this mean in practice?

Needless to say that this obligation is very vague and many controllers will rightfully wonder what measures they would be expected to implement. The GDPR itself provides very little guidance in this regard.

Article 24(2) provides that controllers should implement appropriate data protection policies where proportionate in relation to processing activities. Implementing those policies alone will certainly not achieve compliance with the accountability obligation. Rather, controllers will be required to implement a range of measures as needed to ensure compliance with all of their obligations under the GDPR. In addition, they must implement measures enabling them to objectively demonstrate such compliance. This requirement will need close consideration in practice. Controllers will need to thoroughly document their data protection efforts and, if requested, make such documentation available to authorities. Any data protection measures implemented will also need to be periodically reviewed and updated as appropriate.

Article 24(3), supplemented by Recital 77, provides that adherence to approved codes of conduct and certification mechanisms may help demonstrate compliance with the accountability obligation. Hence, controllers can expect codes of conducts and certification mechanisms to specify the measures required in order to comply with their accountability obligations.

Further guidance on the implementation of appropriate measures and the demonstration of compliance, including on how to identify, assess and mitigate risks associated with data processing, can also be expected from the EDPB.

(b) Accountability and the risk-based approach

The accountability provision is qualified by the so-called risk-based approach: what measures will be appropriate in each case, will depend on the nature, scope, context and purposes of the relevant processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals.

The more likely and severe the risks from the proposed processing, the more measures will be required to counteract those risks. According to Recital 75, processing which could lead to physical, material, or non-material damage would be particularly likely to constitute 'risky' processing requiring particular attention. Recital 75 further provides the following examples as potentially risky processing:

- processing that may give rise to discrimination, identity theft or fraud, financial loss, reputational damage, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;
- processing that might deprive data subjects of their rights and freedoms or prevent them from exercising control over their personal data;
- processing of sensitive personal data or data relating to criminal convictions or offences;
- processing for purposes of profiling;
- processing of personal data of vulnerable natural persons, in particular of children; and
- processing involving a large amount of personal data and affecting a large number of data subjects.

According to Recital 76, the risk must be assessed in an objective manner to determine whether there is a "risk" or a "high risk".

Further guidance on identifying and assessing risks of data processing and on identifying best-practice approaches to mitigate those risks will likely be provided by way of approved codes of conducts, approved certifications and guidelines issued by the Art. 29 Working Party/ EDPB.

Controllers undertaking the types of processing activities listed above or otherwise identified as 'risk' or 'high risk' would be prudent to carefully consider their obligations under the accountability provision.

4. Accountability and existing regulator guidance

Privacy regulators around the world are increasingly embracing the notion of accountability as a vehicle to drive privacy compliance within organisations (regardless of whether their laws currently codify the accountability principle). So far, the privacy regulators in Canada, Hong Kong, France, Australia and Colombia have issued "Accountability Guides" or "Privacy Governance Frameworks" intended to assist private sector (and in some instances, also public sector) organisations setting up appropriate processes and procedures to ensure privacy compliance. In the EU, the EDPS in February 2018 issued guidance on accountability for EU institutions, bodies and agencies.

Those documents have a lot in common and provide helpful (non-binding) guidance. The common thread in existing guidance is that organisations are expected to take a more proactive, systematic and comprehensive approach to privacy compliance. Some of the regulators go as far as to promote privacy management programs as the appropriate tool to ensure privacy compliance. To read more about the rise of the accountability principle and related regulator guidance, please refer to our "Accountability Series" on b:INFORM.[11]

5. Your Accountability Game Plan

Complying with the GDPR accountability provision is a complex task. The very basic Article 24 does not do justice to the overarching concept of accountability which essentially requires controllers to perform all of their data processing operations in compliance with the GDPR and to be able to objectively demonstrate such compliance.

(a) **A best-practice approach** for organisations would be to build and implement a comprehensive privacy management program. In a nutshell, this would include implementing:

- an internal governance structure which fosters a culture of privacy within the organisation from the top down;
- various adequate program controls to ensure compliance with the various GDPR requirements (such as personal data inventories/ records of processing activities, tailored privacy policies and notices, data breach handling procedures, security and retention policies, privacy enhancing measures by implementing data protection by design or by default when building new products or services, conducting data protection impact assessments when the processing is likely to result in a high risk, processes for selecting and managing data processors, etc.);
- processes to continuously monitor, assess and revise the effectiveness and appropriateness of the program controls.

(b) Those organisations wanting to start on a smaller scale (due to lack of resources or other reasons), would be well advised to take the following steps as a starting point:

- consider if they have the right level of expertise, training and a sufficiently senior individual accountable for data protection compliance within the organisation;
- put in place appropriate data protection policies addressing the key requirements under the GDPR;

[11] http://www.bakerinform.com/home/2015/10/10/accountability-a-global-standard?rq=accountability

- implement mechanisms such as spot checks or audits to monitor compliance with those data protection policies;
- devise processes for periodically reviewing and evaluating the effectiveness of data protection policies in place;
- document all of the above to be able to objectively demonstrate upon request their accountability in an organised and effective manner and in a way that is not disruptive to business operations; and
- follow any practical guidance from European authorities on the accountability requirements.

* * * * *

Please contact your usual Baker McKenzie contact for a demo of our information governance tool iG360 designed to help in implementing a comprehensive privacy management program or for support in addressing your accountability obligations.

Game Changer 10: EU Data Protection Officer - Must Have, Nice to Have or Safe to Ignore?

Under the GDPR, certain private and most public sector organisations will be required by law to appoint a data protection officer ("**DPO**") to oversee their data processing operations. The agreed compromise version of the DPO requirement is a DPO requirement 'lite' compared to what the EU Commission and Parliament had originally proposed.

1. Key Takeaways

(a) Virtually all **public sector bodies** will be required to designate a DPO under the GDPR.

(b) When it comes to the **private sector**, the GDPR introduces a limited mandatory DPO requirement. Controllers and processors will only be required to designate a DPO if their core activities consist of:

i. processing operations which, by virtue of their nature, scope and/or purposes, require **regular and systematic monitoring of data subjects on a large scale**; or

ii. processing on a large scale of **special categories of data or data relating to criminal convictions and offences**.

(c) That said, **Member States are free to introduce broader national DPO requirements**.

(d) Even if not required to designate a DPO, multinationals operating across the EU would be well advised to **consider appointing a DPO on a voluntary basis** as this might be the most effective and efficient way to discharge their comprehensive GDPR compliance obligations.

(a) Organisations will have **substantial discretion in designing and implementing their DPO strategy** and would be wise to thoroughly consider available options.

2. Status quo

The Directive does not provide for a mandatory DPO appointment. However, it does stipulate that Member States may provide exemptions or simplifications to notification requirements for controllers who have appointed a "data protection official" in compliance with applicable national law (Article 18, Recital 49). Consequently, most national data protection laws across the EU do not mandate the appointment of a DPO.

The exceptions are Germany and Croatia both of which contain a general, non-sector specific, mandatory DPO requirement which widely applies to private and public organisations in those countries (exempting only very small organisations). Further, a handful of countries contain sector-specific DPO requirements. For example, in Finland, social welfare and healthcare service operators must appoint a DPO, while in Hungary financial institutions, public utility companies and telecoms companies must do so. In addition, other EU countries, including the Netherlands, Luxembourg, Poland and Sweden, provide for voluntary DPO appointments. These appointments (e.g., the Netherlands and Sweden) can exempt the relevant organisation from certain compliance obligations such as prior notification of new processing operations to supervisory authorities (as stipulated in the Directive).).

3. The new Pan-European DPO requirement

(a) Who must designate a DPO?

Private-sector controllers and processors must designate a DPO if their core activities consist of:

- processing operations which, by virtue of their nature, scope and/or purposes require regular and systematic monitoring of data subjects on a large scale; or

- processing on a large scale of special categories of data and data relating to criminal convictions and offences.

In its guidelines on DPOs ("DPOs Guidelines"[12]), the Article 29 Working Party ("WP29") has specified that "core activities" include key operations necessary to achieve the business goals and activities inextricably linked to the core activities (e.g., processing patients' data is inextricably linked to a hospital's core activity of providing health care). "Large scale" should be determined on a case-by-case basis considering the number of data subjects, the volume of data and/or the range of different data items, the duration and geographical extent of processing. "Regular monitoring" is interpreted to mean ongoing or occurring at particular intervals for a particular period, recurring or repeated at fixed times; or constantly or periodically. "Systematic monitoring" is given if monitoring occurs according to a system; is pre-arranged, organized or methodical; is part of a general plan for data collection; or carried out as part of a strategy.

All public authorities or bodies, except courts acting in their judicial capacity, must designate a DPO.

Further, controllers and processors must appoint a DPO as mandated by Union or Member State law. This appears to be a blanket permission for Member States to require DPO appointments beyond what is required under the GDPR and seems very much at odds with the idea of harmonisation pursued with the GDPR. While some Member States may not make use of this discretion, Germany, where currently virtually every business is required to appoint a DPO, retains its broad DPO requirement (i.e., when at least ten persons deal with the automated processing of personal data). An area to watch!

Finally, the GDPR allows for voluntary DPO appointments where no such appointment is mandated. The WP29 is of the opinion that where a voluntary DPO is designated, GDPR requirements apply as if the designation had been mandatory. Therefore, organisations that - although being under no obligation to appoint a DPO - want to establish or maintain privacy-related roles, should avoid confusion with job titles and make clear, internally and externally, that such roles are not DPOs.

(b) What are the requirements for the DPO?

Organisations are free to choose whether to appoint an internal or external DPO. Further, DPOs do not have to exclusively work in their DPO capacity. Rather, they may also perform other tasks as long as that does not result in a conflict of interest and provided that the other tasks (even if not conflicting) leave the DPO enough time to perform the obligations as DPO (i.e., a "pro forma" appointment would not be sufficient in cases where the GDPR provides for a mandatory DPO).

A group of undertakings such as a corporate group may appoint a single DPO provided that he/she is easily accessible from each establishment. According to the WP29, this implies that a DPO must be in a position to:

- efficiently communicate (face-to-face or remotely) with data subjects and cooperate with the data protection authorities concerned; and

- communicate in the language or languages used by the supervisory authorities and the data subjects concerned (with the help of a team if necessary). This requirement appears to be quite challenging for large multinational organisations and it must be seen if and to what extent the WP29 will maintain it.

[12] Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers ('DPOs')' adopted on 13 December 2016 and were last revised and adopted on 5 April 2017 by the Article 29 Working Party.

As regards the qualifications of a DPO, the GDPR is not very prescriptive. It only broadly requires DPOs to possess the professional qualities and expert knowledge of data protection law and practice enabling them to fulfil their role. The WP29 has specified that:

- the level of expertise depends on sensitivity, volume and complexity of data processed and whether data transfers are systematic or occasional; and
- the DPO should have in-depth understanding of GDPR and expertise in national and EU laws, knowledge of the business sector of the organisation and sufficient understanding of processing operations, information security and information systems.

(c) What are the tasks of the DPO?

At a minimum, and having regard to the risks associated with the processing operations, the DPO shall:

- inform and advise the controller/ processor and their employees involved in data processing of their obligations under the GDPR and other data protection laws;
- monitor compliance with the GDPR and other applicable data protection laws as well as with internal data protection policies (including assigning internal data protection responsibilities, training staff and conducting compliance audits);
- provide advice in relation to data protection impact assessments ("DPIA");

It is recommended to seek the advice of a DPO also on the following issues:

- whether or not carry out a DPIA; what methodology to follow when carrying out a DPIA; whether to carry out the DPIA in-house or outsource it; what safeguards to apply to mitigate risks; whether or not the DPIA has been carried out correctly and whether its conclusions are GDPR compliant;
- cooperate with, act as point of contact for, and as appropriate, consult with, supervisory authorities; and
- provide guidance on the implementation of appropriate technical and organizational measures.

(d) What are the controller's/ processor's obligations in relation to the DPO?

The controller/ processor must:

- ensure that the DPO is involved in all data protection issues properly and in a timely manner (i.e., at the earliest stage possible in all issues relating to data protection);
- provide the resources necessary for the DPO to perform his/her tasks, access to personal data and processing operations and maintain his/her expert knowledge;
- ensure that the DPO exercises his/her functions independently and reports to the highest level of management;
- ensure that the DPO does not receive instructions regarding the exercise of his/her tasks as DPO;
- not dismiss or penalise the DPO for performing his/her tasks;
- ensure that data subjects may contact the DPO with regard to all issues related to the processing of their personal data and to exercise their rights; and

- provide the contact details of the DPO when communicating with the supervisory authority, in the records of processing activities and in case of a data breach.

The WP29 has clarified that the controller or processor remains responsible for GDPR compliance and the DPO must be enabled to express their dissenting opinion where this is not followed. Where the controller or processor does not follow the DPO's advice on a DPIA, they should record the relevant justification in the DPIA documentation.

(e) What are the fines for non-compliance?

Failure to comply with the DPO requirements set out in the GDPR may result in administrative fines of up to EUR 10,000,000, or in case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

(f) DPO requirement 'lite'?

The DPO requirement was one of the most controversially debated concepts during the GDPR negotiation process. The European Commission, Parliament and Council had put forward three very different proposals. While the Commission proposed that (amongst others) all private sector controllers/ processors with more than 250 employees should be required to appoint a DPO, Parliament suggested that the key trigger for a DPO requirement be the number of data subjects in relation to which a controller/ processor processed personal data. The Council, on the other hand, rejected a mandatory DPO appointment altogether except where required by Union or Member State law.

What we are left with in the final text of the GDPR is a wide DPO requirement for the public sector on the one hand and a narrow DPO requirement for the private sector on the other hand as well as room for Member States to enact their own broader DPO requirements. It looks like the negotiators settled on a compromise in which the Council very much retained the upper hand.

It appears that the majority of businesses may not be required to appoint a DPO (assuming most Member States refrain from introducing broader DPO requirements and in light of the fact that under the GDPR no incentives are triggered by voluntary DPO appointments). The exception will be businesses regularly processing sensitive information (such as businesses operating in the health sector) and businesses engaging in profiling and other extensive monitoring activities, for which the appointment of a DPO is mandatory.

4. Your DPO Game Plan

We recommend a three-tier Game Plan to get on top of the DPO requirement:

(a) Assess whether or not you will fall within the mandatory DPO requirement.

(b) If yes - consider how best to comply with this requirement.

(c) If no - consider whether your organisation would benefit from a voluntary (maybe temporary) DPO appointment.

(1) Do I fall within the DPO requirement?

Despite the fact that the private-sector DPO requirement is narrow in scope, businesses would be wise to consider whether they fall within the scope of the DPO requirement. As a rule of thumb for private-sector organisations:

- If your organisation does not engage in regular and systematic monitoring of data subjects or process substantial amounts of sensitive data or data relating to criminal convictions or offences, it is unlikely to be required to appoint a DPO.

- If your organisation does engage in regular and systematic monitoring of data subjects or processes substantial amounts of sensitive data or data relating to criminal convictions or offences, a more thorough assessment will be required to determine whether those processing activities form part of the organisation's core (i.e., primary) activities and whether or not the processing occurs on a large scale. If the answer to those questions is 'yes', a DPO will likely need to be appointed.

Businesses should also consult Member State law and, if there is still doubt, the competent supervisory authority or legal counsel to confirm whether a DPO must be appointed.

(2) If I fall within the DPO requirement, how do I best comply with it?

If your organisation is caught by the DPO requirement, you should develop a compliant DPO strategy which minimises any negative operational impact (e.g., costs, business disruption) and maximises operational gain (e.g., streamlined processes and systems, reputational benefits).

Key questions to consider and decisions to make include:

(a) Should we appoint an internal or external DPO? Obviously, costs will come into play. But other factors should also be considered. For example, an internal on-premise DPO would likely have a better understanding of the business and better relationships with relevant employees, while an external DPO might have the advantage of being able to draw on experiences from working with other businesses, and the organisation could shift responsibility for data protection compliance to an external service provider.

(b) If we appoint an internal DPO, should this person act exclusively as DPO or can he/she perform the DPO role in addition to other tasks? An 'exclusive' DPO will obviously be in a much better position to discharge the DPO duties but this might not be necessary in all cases (provided no conflict of interest exists). Further, the associated costs might be a prohibitive factor. When looking at the DPO's overall tasks (i.e., those acting exclusively as DPO and those in other roles) in cases where a DPO appointment is mandatory, organisations must ensure that - from a de facto point of view - the sheer total number of tasks and responsibilities does not lead to inhibiting the DPO from performing the DPO tasks.

(c) Should we appoint just one DPO for a group of undertakings, and if yes, in which country? Accessibility of the DPO across the various undertakings as well as the existing structures, processes and synergies between various relevant establishments will be a key consideration here. The more integrated a group of undertakings and, correspondingly, the less relevant the structure provided by the legal entities is (e.g., because of matrix structures and divisional company structures), the greater the advantage in appointing a group-wide DPO. A centrally appointed DPO, in an integrated organisation, can be very effective in implementing group-wide strategies, concepts, policies, notices and other privacy compliance tools. However, the WP29 has also issued guidance stating that the central DPO must be able to communicate in the language or languages used by the supervisory authorities and the data subjects concerned. This may be challenging if many countries and languages are concerned.

(d) Can we draw on existing personnel and experience? If your organisation has a DPO in place already (whether on a European or local level), that person is likely to satisfy the new EU-wide DPO requirement, subject to maybe a few adjustments. If nothing else, that person will likely be a good source of knowledge.

(e) How do we structure reporting lines and integrate the DPO with other business functions? It is a pre-requisite for the DPO to report directly to the highest management of the appointing body. While this reporting requirement is mandatory, in practice there are often additional reporting requirements imposed on the DPO in order to preserve a homogenous level of knowledge within the organisation (especially at the level of the privacy-enabling functions drafting contracts, notices etc.) or the group of companies. As regards reporting lines to the DPO, the GDPR is silent. But to enable the DPO to discharge his/her duties, it will be indispensable to establish direct reporting lines to him/her from various business functions (e.g.,

marketing, HR, finance, etc.) and, especially where a group-wide DPO is in place, from the DPO's local privacy coordinators (i.e., from the various group companies' employees who have privacy compliance-related tasks despite not being appointed as DPOs).

(3) If I don't need to appoint a DPO, should I do it anyway?

Even if organisations are not required to appoint a DPO, doing so might be beneficial for many reasons. To name just a few, appointing an experienced and business-savvy DPO (even on a temporary basis):

- might be the most practical and cost-efficient solution to achieve GDPR compliance - remember, even if the DPO appointment does not apply to your organisation, various other GDPR requirements are very likely to apply;
- will most likely put you in a better position when negotiating privacy-relevant contracts or when dealing with supervisory authorities; and
- will streamline and optimise your privacy-relevant processes across the EU allowing your other personnel to focus on revenue-raising and other key tasks.

However, organisations which are not obliged to designate a DPO should be mindful that GDPR requirements on DPO will apply to voluntary DPOs. Therefore, these organisations may decide to assign a privacy-related job title different from DPO to avoid being unnecessarily subject to the relevant GDPR requirements. Organisations might need to take the protection against dismissal of already appointed DPOs in certain Member States (e.g., Germany) into account, when appointing a new (group-wide) DPO.

* * * * *

Please contact your usual Baker McKenzie contact for assistance in assessing whether or not your organisation must or should appoint a DPO and, if so, in devising a DPO solution that best fits with your organisation's needs and structures.

Game Changer 11: Cross-Border Data Transfer Rules under the GDPR

Designing and implementing a privacy-compliant cross-border data transfer strategy is a complex and challenging task. It requires a thorough analysis of one's data flows, as well as the applicable legal frameworks, which vary between countries and are generally complex sets of rules. It further requires a complicated risk assessment to determine if the proposed transfers will provide an adequate level of protection for the rights of the data subjects or if additional safeguards are required.

As cross-border data transfers are poised to remain a top priority for EU privacy regulators in the foreseeable future, businesses would be prudent to start the (potentially lengthy) process of designing and implementing a GDPR compliant cross-border data transfer strategy now.

1. Key Takeaways

(b) **In principle, the GDPR will retain the cross-border data transfer rules of the Directive**: data may be transferred out of the EU/EEA only to countries which have been recognised as providing an adequate level of data protection, unless the transferor can rely on specific derogations or adduces specific additional safeguards ensuring an adequate level of data protection.

(c) Subject to the changes listed under (d) below, the list of **available derogations and options for adducing additional adequate safeguards** will remain the same.

(d) Adequacy decisions and standard contractual clauses issued by the Commission under the Directive as well as BCRs and contractual clauses approved by national supervisory authorities under the Directive **will remain valid unless and until formally amended, replaced or repealed**.

(e) **Noteworthy changes to the cross-border data transfer rules** include the following:

(i) Transfers will no longer be subject to country-specific authorisation processes except that transfers based on contractual clauses which have not been adopted or approved by the Commission will require specific supervisory authority approval.

(ii) Adequacy decisions will be subject to clearer and more prescriptive standards as well as regular review and may be made in relation to territories and industry-sectors within a country.

(iii) The GDPR offers certification mechanisms and codes of conduct as additional options for adducing appropriate safeguards.

(iv) BCRs will be formally recognised as measures adducing appropriate safeguards and will be subject to uniform rules when it comes to their adoption.

(v) Approved standard contractual clauses may be supplemented with additional clauses or safeguards subject to certain conditions.

(vi) Transferors wanting to rely on consent as a derogation will need to inform the data subject about the risks resulting from the transfer before obtaining his/her explicit consent.

(vii) The GDPR will introduce one new but very limited derogation which may help legitimise occasional transfers which are small in scope and would otherwise be prohibited.

2. The status quo

All EU countries currently restrict data transfers to countries outside the European Economic Area ("**EEA**"). While differences exist between the various national restrictions (e.g. some states require prior

notification or even authorisation of those transfers while others don't), broadly speaking the transfer rules are largely the same across the EU/EEA.

As a general rule, the Directive prohibits transfers of personal data from within the EU to countries outside the EEA unless those countries ensure an adequate level of privacy protection. However, this rule is subject to exceptions, including that the transfer of data to third countries not offering an adequate level of privacy protection is permitted if the controller adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals or can rely on one or more available derogations.

2. The new scheme

In principle, the GDPR retains the data transfer rules of the Directive.

(a) Transfers with an adequacy decision

As a general rule, personal data may be transferred to a third country or international organisation where the Commission has decided that the third country, or a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. In these cases, no specific authorisation of the transfer by supervisory authorities ("SAs") will be required.

While this general rule is similar to what we have under the Directive, there are some noteworthy changes, some of which are - no doubt - a reaction to the *Schrems* judgment. In particular:

- Not only a third country but also territories or industry-sectors within a country as well as international organisations may be given adequacy status. For example, single U.S. States with comprehensive privacy legislation or heavily regulated sectors in a country (such as the financial or health sector in the U.S.) may be given adequacy status.

- The rules for assessing the adequacy of the level of privacy protection in a given country, territory, sector or international organisation are much more prescriptive than those under the Directive. Importantly, in order to be given adequacy status, a third country is expected to offer guarantees that ensure a level of data protection essentially equivalent to that guaranteed within the EU. In particular, it should ensure effective independent data protection supervision and provide for cooperation mechanisms with European SAs. Further, data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

- Adequacy decisions will be subject to a periodic review and may be repealed, amended or suspended by the Commission if the latter concludes that an adequate level of data protection is no longer ensured.

- Importantly, adequacy decisions issued under the Directive will remain in force until amended, replaced or repealed by the Commission pursuant to the mechanisms provided by the GDPR.

(b) Transfers by way of appropriate safeguards

In the absence of an adequacy decision, controllers and processors may transfer personal data outside the EEA if they have adduced appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Those safeguards are intended to ensure that, post-transfer, the data is processed in compliance with data protection requirements of European standard and data subjects have the same rights as they have in the European Union. Such safeguards should also cover onwards transfers.

The GDPR provides for two types of appropriate safeguards - those that do not require specific authorisation from a supervisory authority and those that do require such authorisation.

Appropriate safeguards that do not require specific SA authorisation are:

- Binding Corporate Rules ("BCRs") which are now expressly recognised as a legitimate transfer tool subject to complying with detailed requirements;
- standard data protection clauses adopted by the Commission, or adopted by a SA and approved by the Commission;
- approved codes of conduct or approved certification mechanisms, in each case together with binding and enforceable commitments of the controller/ processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; and
- legally binding and enforceable instruments between public authorities or bodies.

Appropriate safeguards that do require specific SA authorisation are:

- contractual clauses between the controller/ processor on the one hand, and the controller/ processor/ recipient of the data in the third country or international organisation on the other hand; and
- provisions to be inserted into administrative agreements between public authorities or bodies which include enforceable and effective data subject rights.

Key changes to note include:

- BCRs are now formally recognised across the EU and will be subject to more harmonised rules easing the compliance burden for companies.
- The GDPR offers some welcome flexibility with respect to approved standard contractual clauses. These may now be supplemented with additional clauses or safeguards as long as these do not contradict the approved standard contractual clauses or prejudice the fundamental rights and freedoms of the data subjects. Unlike under the Directive, such changes will not transform standard contractual clauses into non-standard contractual clauses.
- The newly introduced possibility to adduce appropriate safeguards to legitimise data transfers through approved codes of conduct and certification mechanisms adds a new dimension to data transfers. Essentially, the third country recipient of the data would need to make a binding and enforceable commitment to adhere to the standards laid down in those codes of conducts or certification schemes and would then be considered to offer appropriate safeguards required to legitimise the transfer.

It is also worth noting that standard contractual clauses approved by the Commission under the Directive as well as data transfers authorised by national SAs on the basis of additional safeguards (such as contractual clauses or BCRs) will remain in force under the GDPR unless formally amended, repealed or replaced.

(c) Derogations for specific situations

In the absence of an adequacy decision or appropriate safeguards, personal data may be transferred out of the EU only if:

- the data subject has explicitly consented to the proposed transfer after having been informed of the possible risks of such transfer;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;

- the transfer is necessary for important reasons of public interest (e.g., data may need to be exchanged internationally between competition or financial supervisory authorities or for public health matters);

- the transfer is necessary for the establishment, exercise or defence of legal claims;

- the transfer is necessary in order to protect the vital interests (including physical integrity or life) of the data subject or other persons where the data subject is physically or legally incapable of giving consent; or

- the transfer is made from a public register and certain other conditions are fulfilled.

The above derogations largely mirror those provided for in the Directive, except that consent is now required to be explicit and the data subject must be informed about the risks resulting from the transfer prior to consenting.

The GDPR also provides for one new very limited "last resort" derogation. Essentially, if a proposed transfer cannot be based on an adequacy decision, appropriate safeguards or one of the above derogations, a transfer may take place if it is not repetitive (i.e., occasional), concerns only a limited number of data subjects and is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject. But, as a further condition, the controller must adduce suitable safeguards to protect the personal data (having assessed all the circumstances surrounding the data transfer) and inform the SA and the data subjects about the transfer.

3. Your cross-border data transfer Game Plan

To get on top of your cross-border data transfers and ensure they are GDPR compliant, we recommend the following Game Plan:

(a) Identify and map out your data flows to get a clear picture of what data flows, from where, to which recipients, in which countries (see our article on Data Mapping in this booklet for further information).

(b) Design a comprehensive strategy which will legitimise all of those transfers. This will require you to:

(i) identify the available option(s) for legitimising your various data flows out of the EEA (i.e., can you rely on adequacy decisions or derogations or are additional safeguards required?). This will require a complex risk assessment of your current and proposed data flows taking into account the data protection frameworks of various countries involved;

(ii) assess whether it makes sense to change/ streamline some of your data flows to reduce the compliance burden (e.g., would it make sense to keep certain data within the EEA or send it to fewer/other countries?);

(iii) assess whether your current transfer mechanisms, such as consent, should be retained and/or will need to be adapted or added to in order to remain compliant under the GDPR; and

(iv) consider more comprehensive transfer mechanisms such as BCRS which may appear burdensome and costly in the short-term but might be the most efficient and reliable solution in the long-term.

(c) Continuously map your data flows and assess them against your transfer strategy and periodically review your transfer strategy in order to ensure compliance in the long-term.

* * * * *

Please contact your usual Baker McKenzie contact for assistance in assessing your current data transfer strategy and/or designing and implementing a GDPR compliant cross-border data transfer strategy.

Game Changer 12: New Pan-European Data Breach Notification Obligations

A key change under the GDPR will be the introduction of general (non-sector specific) data breach notification obligations. Subject to limited exceptions, data controllers will be required to notify personal data breaches to the competent supervisory authority ("**SA**") and, in certain cases, also to affected data subjects.

The pan-European data breach notification scheme is set to become a major compliance hurdle for organisations operating within the EU. Businesses are well advised to treat this as a compliance priority.

1. Key Takeaways

(a) Controllers must **notify a personal data breach to the competent SA without undue delay** and, where feasible, not later than 72 hours after having become aware of it unless the breach is unlikely to result in a risk for the rights and freedoms of individuals.

(b) Subject to limited exceptions, controllers must **communicate a personal data breach to data subjects without undue delay** if the breach is likely to result in a high risk for their rights and freedoms.

(c) Organisations will need to put in place **data breach incident management plans** and **update their controller/ processor contracts**.

(d) Non-compliance exposes organisations to **substantial fines and damage to reputation**.

2. The status quo

The Directive does not require Member States to impose data breach notification obligations. As a consequence, to date most EU Member States have not implemented mandatory data breach notification schemes (except with respect to providers of publicly available electronic communication services). The exceptions are Germany, Austria and, since 1 January 2016, The Netherlands, each of which have each enacted non-sector specific mandatory data breach notification legislation.

3. The new scheme

The GDPR adopts a two-tier approach setting a lower threshold for notification to supervisory authorities ("**SAs**") than for notification to affected individuals. In the following, unless expressly referred to a processor, the obligations apply to controllers.

(a) When do I have to notify the SA?

Controllers must notify a personal data breach to the competent supervisory authority unless the breach is unlikely to result in a risk for the rights and freedoms of individuals. Importantly, those breaches that are unlikely to result in a risk for the rights and freedoms of individuals are exempt from the notification obligation providing some discretion for controllers to assess whether or not a breach must be reported. However, this exemption should be interpreted narrowly and would require the controller to demonstrate - in accordance with the accountability principle - that the breach is unlikely to result in a risk for the rights and freedoms of individuals.

(b) When do I have to notify affected individuals?

Data breaches must also be communicated to affected data subjects if they are likely to result in a high risk for their rights and freedoms.

Importantly, notification to data subjects is not required if:

- the controller adequately secured the relevant data by implementing appropriate technical and organisational protection measures (such as encryption) in relation to it;
- following the breach, the controller has taken measures to ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialise; or
- the notification of individual data subjects would require disproportionate effort - in this case a public communication of the breach would be required though.

The DPA also has the power to order controllers to communicate a personal data breach to data subjects.

(c) What is a "personal data breach"?

"Personal Data Breach" is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

(d) What are the timeframes for notification?

Organisations must notify data breaches to the SA without undue delay and, where feasible, not later than 72 hours after having become aware of it.

Processors that become aware of a data breach must notify the relevant controller of the breach without undue delay.

Affected data subjects must be notified without undue delay. While this timeframe might sound quite lax, affected individuals should be notified as soon as reasonably feasible and in line with any guidance provided by the notified supervisory authority.

(e) What information must be included in the notification?

The notification to the SA must contain certain prescribed information, such as the nature and scope of the breach as well as the likely consequences and measures taken or proposed to address the breach. If it is not possible to provide all this information at the same time, the information may be provided in phases without undue delay but an explanation for the delay should be provided.

Notifications to affected data subjects must essentially communicate the same information but also offer some recommendations to the individuals as to how to mitigate potential adverse effects of the breach. Further, the notification must be in clear and plain language..

(f) Any other obligations?

Controllers must also document any data breaches.

(g) What are the applicable sanctions?

Failure to notify data breaches as required may lead to administrative fines of up to EUR 10,000,000, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year (whichever is higher). Non-compliance with an order by the DPA to notify data subjects may lead to administrative fines of EUR 20,000,000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover (whichever is higher).

Further, data subjects will be entitled to receive compensation for any damage suffered from the breach.

4. Practical challenges

While the notification obligations as prescribed in the GDPR may appear quite straightforward, in practice, many breach scenarios will not be clear-cut and will require a close case-by-case consideration as well as collaboration with, and guidance from, SAs.

Many questions will arise, some of which may not be easy to answer, such as:

(a) **Did a data breach occur?** Considering that many organisations do not even become aware of data breaches within their organisation for months or even years after they occurred, this threshold question will pose considerable challenges in practice.

(b) **If a breach occurred, will it need to be reported, and if so, to whom?** This will require a thorough risk-assessment. The necessary relevant circumstances to take into account will include the nature and gravity of the breach, the likely adverse consequences of the breach (such as identity theft or fraud, financial loss, damage to reputation, etc.) as well as security measures implemented in order to protect the relevant data.

(c) **Within which time frame will a breach need to be reported?** This will require an understanding as to when an organisation will be considered to be "aware" of a breach.

(d) **How much information do I need to disclose in the notifications?** The information which must/ should be disclosed will always require a careful analysis of the individual circumstances, the legal requirements and any conflicting interests.

(e) **What measures to mitigate risks can be taken following a breach?** Again, a thorough risk-assessment and balancing of interests will be required in order to come up with feasible and cost-effective solutions.

5. Your data breach notification Game Plan

No doubt organisations will need to take a proactive, rather than reactive, approach to this obligation. To meet compliance with the new European data breach notification obligations, organisations will need to:

- put in place a sound Data Breach Incident Management Plan ("DBIM Plan"); and
- reflect data breach reporting obligations in controller/ processor contracts.

(a) DBIM Plans

DBIM Plans will require time and careful planning. Plans need to be tailored to the specific organisation, assign responsibilities and prescribe clear processes and procedures for dealing with suspected data breaches.

When designing European DBIM Plans, multinationals should also keep an eye on their data breach response strategies in other jurisdictions. Mandatory data breach notification schemes are being introduced across the globe as effective privacy compliance drivers. While the notification triggers, time frames and formats may vary between jurisdictions, data breach notification obligations are becoming a global norm and increasingly warrant a global approach and response. If nothing else, existing DBIM Plans for other jurisdictions might provide useful reference points for any European version.

(b) Controller/ processor contracts

In relation to controller/ processor contracts, these will likely need to be updated to require processors to notify data breaches to controllers in a timely manner. From a controller point-of-view, clear parameters should be stipulated for processors, including a requirement to provide the assistance necessary to the controller to ensure the controller will be able to discharge its

notification obligations. From a processor point-of-view, notification obligations should not go beyond what is necessary and manageable.

* * * * *

Please contact your usual Baker McKenzie contact for assistance in designing, implementing or testing your DBIM plan or for support with updating your controller/ processor contracts.

Game Changer 13: Enforcement and Sanctions under the GDPR

The new enforcement and sanction powers granted to supervisory authorities ("**SAs**") under the GDPR, including the new significant fines that may be imposed for GDPR violations, are likely the GDPR Game Changer most feared by organisations. The new enforcement and sanctions regime will, no doubt, focus management attention and push data protection compliance further up on the risk agenda for many organisations.

1. Key Takeaways

(a) Unlike the Directive, the GDPR **describes in great detail the measures and procedures for enforcement** leaving very little discretion to Member States to make up their own rules.

(b) **SAs across all Member States will have the same powers**, including investigative powers, corrective powers and sanctions, as well as powers to bring infringements of the GDPR to the attention of judicial authorities and/or engage in legal proceedings to enforce the provisions of the GDPR.

(c) **The imposition of fines is likely to become the norm** as the GDPR states as a general rule (subject to very limited exceptions) that penalties and administrative fines should be imposed for any infringement of the GDPR in addition to, or instead of, appropriate measures imposed by the SA.

(d) **The GDPR sets the upper limit and criteria for determining fines** which are then finally determined by the competent SA in each individual case having regard to a variety of factors and circumstances listed in the GDPR.

(e) The **maximum applicable fines** are:

- in cases of major infringements (such as failure to comply with cross-border transfer rules or obtain adequate consents) **EUR 20,000,000**, or in the case of an undertaking, up to **4% of the worldwide annual turnover of the preceding financial year** (whichever is higher); and
- in cases of other infringements (such as failure to appoint a DPO as mandated or comply with the requirements for appointing a processor) **EUR 10,000,000**, or in the case of an undertaking, up to **2% of the worldwide annual turnover of the preceding financial year** (whichever is higher).

(f) In the case of an undertaking, the worldwide annual turnover relevant for determining the amount of the fine may be the **turnover of a parent company** if that is held liable for the infringement (even if the parent did not actively participate in the infringement).

(g) Member States may provide that certain **non-profit bodies**, **organisations or associations may** (i) **exercise certain data subjects' rights on their behalf** (such as the right to lodge complaints with SAs or seek judicial review in cases of alleged GDPR infringements), and/ or (ii) **lodge a complaint or take legal action against supervisory authorities or controllers/ processors independently of a data subject's mandate** if they consider that data subjects' rights have been infringed as a result of non-compliant processing. These rights are likely to add an additional dimension to data protection enforcement if taken up by a number of Member States.

(h) In view of the significant fines, organisations of all sizes would be **wise to get their privacy house in order**, focusing:

- as a **first step** on high-risk areas such as cross-border data transfers, consents and data subjects' rights; and
- as a **second step** on other areas such as implementing appropriate security measures and a data breach incident management plan.

2. Enforcement under the GDPR

The GDPR describes in great detail the measures and procedures for enforcement of the GDPR provisions leaving very little discretion to Member States to make up their own rules. Notably, (as touched on below and discussed in more detail in our Data Processor article in this booklet) under the GDPR both controllers and processors may be subject to direct enforcement action (including fines).

(a) Who is responsible for enforcement?

Each Member State is required to establish one or more independent public authorities responsible for monitoring compliance with, and enforcing the provisions of, the GDPR. The GDPR goes further than that and clarifies that each such supervisory authority should be provided with the financial, human and technical resources, premises and infrastructure necessary for the effective performance of their tasks. Importantly, those supervisory authorities who previously relied on notification fees as a resource will no longer have this income stream available. It remains to be seen whether the GDPR will result in better equipped and more active regulators.

(b) What enforcement powers do SAs have?

The GDPR expressly states that, in order to ensure consistent monitoring and enforcement, SAs should have the same tasks and effective powers across Member States. From an enforcement perspective, these powers include investigative powers, corrective powers and sanctions, as well as powers to bring infringements of the GDPR to the attention of judicial authorities and/or engage in legal proceedings to enforce the provisions of the GDPR. As a general rule, enforcement measures must be appropriate, necessary and proportionate in view of each individual case. SAs have less discretion about enforcement rules, but critically they retain discretion about application of the provisions.

➔ Investigative powers

The SAs investigative powers include, amongst others, powers to:

- order controllers and processors to provide information;
- carry out investigations in the form of data protection audits;
- obtain from controllers or processors access to personal data and other information; and
- obtain access to any controller/ processor premises (which power should be exercised in compliance with national procedural requirements, such as obtaining prior judicial authorisation).

➔ Corrective powers and sanctions

The SAs corrective powers include, amongst others, powers to:

- issue warnings to controllers/ processors that intended processing operations are likely to infringe the GDPR;
- issue reprimands to controllers/ processors where processing operations infringe the GDPR;
- order controllers/ processors to bring processing operations into compliance with the GDPR;
- order controllers to communicate personal data breaches to data subjects;
- impose a temporary or definitive limitation (including a ban) on processing;
- impose administrative fines (in addition or instead of any other corrective measures); and
- order the suspension of international data flows.

(c) Focus: Administrative fines and penalties

In order to strengthen and harmonise administrative penalties for data protection infringements, the GDPR sets the upper limit and criteria for determining fines which are then finally determined by the competent SA in each individual case.

Importantly, the GDPR expressly states that as a general rule (in order to strengthen enforcement of the GDPR rules), penalties and administrative fines should be imposed for any infringement of the GDPR in addition to, or instead of, appropriate measures imposed by the SA. The exceptions are minor infringements and cases in which a fine would constitute a disproportionate burden to a natural person. In those cases, a reprimand may be issued instead of a fine. Therefore, the imposition of fines is likely to become the norm.

(i) Rules for determining administrative fines

The GDPR provides the following rules for determining the scope of administrative fines to be imposed:

- The imposition of administrative fines shall in each case be effective, proportionate and dissuasive.
- Depending on the circumstances of each individual case, administrative fines should be imposed in addition to, or instead of, other corrective measures.
- Various factors need to be considered when determining whether to impose a fine and of what amount, including in particular:
  - the nature, gravity and duration of the infringement;
  - the intentional or negligent character of the infringement;
  - actions taken to mitigate damage suffered;
  - the degree of responsibility or any relevant previous infringements;
  - the manner in which the infringement became known to the SA (in particular whether the controller/ processor notified the SA);
  - the degree of cooperation with the SA in order to remedy the infringement and mitigate the adverse effects;
  - compliance with measures previously ordered against the controller/ processor;
  - adherence to a code of conduct; and
  - any other aggravating or mitigating factors (such as financial benefits gained).
  - If a controller or processor violates several provisions of the GDPR in relation to the same or linked processing operations, the total amount of the fine may not exceed the amount specified for the gravest violation.

(ii) Level of administrative fines

The GDPR imposes a two-tier fine system.

Tier-one infringements are subject to administrative fines of up to **EUR 10,000,000**, or in the case of an undertaking, up to **2% of the worldwide annual turnover of the preceding financial year** (whichever is higher).

Tier-one Infringements	Responsibility on…	
	controllers	processors
▪ failure to obtain parental consent where information society services are offered to children below the age of consent (Art. 8)	✓	X
▪ failure to inform data subjects that personal information about them is de-identified (Art. 11)	✓	X
▪ failure to adhere to data protection by design/data protection by default principles (Art. 25)	✓	X
▪ failure to comply with requirements for joint controller arrangements (Art. 26)	✓	X

Tier-one Infringements	Responsibility on…	
	controllers	processors
▪ failure to designate a representative in the EU in case not established in the EU (Art. 27)	✓	✓
▪ failure to comply with the requirements for appointing and acting as a processor (Art. 28, 29)	✓ (as applicable)	✓ (as applicable)
▪ failure to maintain adequate processing records (Art. 30)	✓	✓
▪ failure to cooperate with SA on request (Art. 31)	✓	✓
▪ failure to implement appropriate security measures (Art. 32)	✓	✓
▪ failure to notify data breaches as required (Art. 33, 34)	✓	X
▪ failure to carry out DPIAs as required or consult with SA on high-risk processing (Art. 35, 36)	✓	X
▪ failure to appoint a DPO (if mandated) (Art. 37, 38, 39)	✓	✓
▪ failure to comply with certification requirements (Art. 42, 43)	✓	✓

Tier-two infringements are subject to administrative fines of up to **EUR 20,000,000**, or in the case of an undertaking, up to **4% of the worldwide annual turnover of the preceding financial year** (whichever is higher).

Tier-two Infringements	Responsibility on…	
	controllers	processors
▪ failure to comply with the basic processing principles, including conditions for consent (Art. 5, 6, 7, 9)	✓	X
▪ failure to comply with data subjects' rights (Art. 12-22)	✓	X
▪ failure to comply with cross-border transfer principles (Art. 44-49)	✓	✓
▪ failure to comply with any obligations adopted pursuant to Member State law (Chapter IX)	✓ (as applicable)	✓ (as applicable)
▪ failure to allow SA access to personal data and/ or premises in order to exercise its investigative powers (Art. 58(1))	✓ (as applicable)	✓ (as applicable)
▪ failure to comply with an order issued by a SA in exercising its corrective powers (Art. 58(2))	✓ (as applicable)	✓ (as applicable)

(iii) Worldwide annual turnover of undertakings

Undertakings may be subject to administrative fines of up to 2% or 4% of the worldwide annual turnover of the preceding financial year. This begs the question what encompasses the "worldwide annual turnover" - is that the relevant turnover of the entity in breach or its entire corporate group? Further guidance is expected from SAs on this.

Recital 150 provides that where fines are imposed on an undertaking, the undertaking should be understood as defined in European competition law provisions.

In the context of determining fines under EU competition law, an "undertaking" refers to the entities that are held liable for the infringement. This may include multiple separate legal entities and, in particular, a parent may be held liable for the actions of a subsidiary if the parent

exercised "decisive influence" over the subsidiary (even if the parent did not actively participate in the infringement). Determining whether a parent exercised decisive influence requires a fact-based analysis (although there is a presumption that a parent will be held liable in respect of its wholly-owned subsidiary). If a parent is held liable then the parent's turnover will be used to calculate the fine, i.e. the 2%/ 4% fine cap will apply to the parent's turnover, thereby significantly increasing the potential level of the fine.

(d) Data subjects' enforcement-related rights

Data subjects also have certain rights in the case of an alleged infringement of the GDPR which controllers and processors should be aware of from an enforcement perspective.

Firstly, data subjects may lodge a complaint with the competent SA in the case of an alleged infringement of the GDPR (and have a right to an effective judicial remedy against the SA if the SA does not deal with the complaint or appropriately inform the data subject on the progress or outcome of the complaint).

Secondly, data subjects have the right to an effective judicial remedy against a controller or processor if they consider that their rights under the GDPR are infringed as a result of a processing of their personal data in non-compliance with the GDPR.

Thirdly, any person that has suffered material or immaterial damage as a result of an infringement of the GDPR is entitled to receive full and effective compensation from the responsible controller or processor.

It should be noted that data subjects may mandate certain non-profit bodies, organisations or associations to exercise the above rights on their behalf if provided for by Member State law (Art.80(1)). Further, Member States may provide that such non-profit bodies, organisations or associations have the right - independently of a data subject's mandate - to lodge complaints with SAs or seek judicial review if they consider that rights of the data subject have been infringed as a result of data processing in breach of the GDPR (Art. 80(2)). Germany, by way of example, has just passed a law giving certain non-profit organisations standing to initiate proceedings for certain data protection infringements. This is expected to significantly increase the number of proceedings for data protection violations against data controllers and processors and will also likely result in more comprehensive corrective measures being imposed on them.

Data subjects shall be entitled to file a claim with a single SA, particularly in the Member State of their residence, workplace or place of the alleged infringement. In practice, this will require all data controllers or data processors having legal defence capabilities in all Member States where they gather personal data.

(e) Room for Member State divergences

The GDPR leaves very limited room for Member States to make up their own enforcement rules. In particular, Member States:

- have discretion to determine whether and to which extent public authorities should be subject to administrative fines (Recital 150, Art.83(7));
- may lay down the rules for criminal sanctions for GDPR infringements (Recital 149, Art.84); and
- may allow for certain non-profit associations to lodge complaints or initiate data protection proceedings, either with or without being asked to do so by affected individuals (as explained above).

To the extent that Member States will have to integrate these enforcement rules within their legal system, the existing differences among them, both at the procedural level and in the way liability is established, can result in significant differences in practice. For instance, the data subject's right to

receive full and effective compensation from the responsible controller or processor may imply much higher amounts in jurisdictions where indirect or punitive damages are recognised.

3. Your Enforcement & Sanctions Game Plan

Both controllers and processors alike will need to get their heads around the new enforcement and sanctions system. We have set out a Game Plan below to help protect your business as much as possible from becoming the target of GDPR enforcement action.

(a) Get your privacy house in order - Obviously, the best way to protect your organisation from substantial fines and other enforcement action is to ensure your business practices are privacy-compliant. This can be a considerable and time consuming task, a sensible approach would be to:

(i) First focus your compliance efforts on those requirements that attract the highest fines in case of non-compliance, such as:

- basic processing principles, including consents (see the article on Consent in this booklet);
- data subjects' rights (see the article on Data Subjects' Rights in this booklet);
- cross-border transfer rules (see the article on Cross-Border Transfers in this booklet);
- orders from SAs (these should be complied with if and when received); and
- certain Member State specific requirements (such as data protection requirements in the employment context).

(ii) As a second step, address remaining compliance requirements such as:

- maintaining adequate processing records (see the article on Data Mapping in this booklet, although data mapping would ideally be your first step in your privacy compliance strategy);
- implementing appropriate security measures;
- appointing a DPO, if mandated (see the article on DPO in this booklet);
- implementing a data breach incident management plan (see the article on Data Breach in this booklet);
- complying with data protection by design and by default principles; and
- carrying out DPIAs.

(b) Be able to demonstrate your level of privacy compliance - An important factor under the GDPR in general and also specifically in relation to fines is the principle of accountability. It not only requires you to implement appropriate technical and organisational measures to ensure that your data processing operations are privacy-compliant. It also requires you to be able to demonstrate such compliance. If you are able to demonstrate a good general level of privacy compliance within your organisation, you will likely receive more lenient treatment from SAs in case of an infringement. So, formalise and document your privacy compliance measures! The overall goal should be the implementation of a formal privacy compliance program with designated responsibilities, management buy-in and specific measures and program controls.

(c) Cooperate with SAs - In case of an infringement, cooperate with the competent SA. For example, make information available to SAs, comply with their guidance and requests, attempt to mitigate any damage suffered by data subjects, and even consider a proactive infringement notification to the SA in certain cases.

* * * * *

Please contact your usual Baker McKenzie contact for help in designing and implementing a comprehensive privacy compliance program or individual privacy compliance measures and to answer any GDPR enforcement questions which you may have.

Baker McKenzie's Global Privacy Team

North America

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

Michael Egan
Partner, Washington, D.C.
+202 452 7022
michael.egan@bakermckenzie.com

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

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

EMEA

Alessandro Celli
Partner, Zurich
+41 44 384 13 66
alessandro.celli@bakermckenzie.com

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

Robbie Downing
Consultant, London
+44 (0)20 7919 1161
robbie.downing@bakermckenzie.com

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

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

Julia Kaufmann
Partner, Munich
+49 89 5 52 38 242
julia.kaufmann@bakermckenzie.com

Holger Lutz
Partner, Frankfurt
+49 69 299 08638
holger.lutz@bakermckenzie.com

Yann Padova
Partner, Paris
+331 4417 5923
yann.padova@bakermckenzie.com

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

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

Matthias Scholz
Partner, Frankfurt
+49 69 2 99 08 180
matthias.scholz@bakermckenzie.com

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

Harry Small
Partner, London
+44 (0)20 7919 1914
harry.small@bakermckenzie.com

Ian Walden
Consultant, London
+44 (0)20 7919 1247
ian.walden@bakermckenzie.com

APAC

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

Kherk Ying Chew
Partner, Kuala Lumpur
+60 3 2298 7933
kherkying.chew@wongpartners.com

Ken Chia
Partner, Singapore
+65 6434 2558
ken.chia@bakermckenzie.com

Patrick Fair
Partner, Sydney
+61 2 8922 5534
patrick.fair@bakermckenzie.com

Adrian Lawrence
Partner, Sydney
+61 2 8922 5204
adrian.lawrence@bakermckenzie.com

Zhenyu Ruan
Partner, Shanghai
+86 21 6105 8577
zhenyu.ruan@bakermckenzie.com

Paolo Sbuttoni
Counsel, Hong Kong
+852 2846 1521
paolo.sbuttoni@bakermckenzie.com

Kensaku Takase
Partner, Tokyo
+81 3 6271 9752
kensaku.takase@bakermckenzie.com

Daisuke Tatsuno
Partner, Tokyo
+81 3 6271 9479
daisuke.tatsuno@bakermckenzie.com

Latin America

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

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

Flavia Rebello
Partner, Sao Paulo
+55 11 3048 6851
flavia.rebello@trenchrossi.com

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

Baker McKenzie.

www.bakermckenzie.com

Our difference is the way we think, work and behave – we combine an instinctively global perspective with a genuinely multicultural approach, enabled by collaborative relationships and yielding practical, innovative advice. Serving our clients with more than 4,200 lawyers in over 45 countries, we have a deep understanding of the culture of business the world over and are able to bring the talent and experience needed to navigate complexity across practices and borders with ease.

Baker McKenzie International is a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a “partner” means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an “office” means an office of any such law firm. www.bakermckenzie.com