Member States' derogations undermine the GDPR

William Long and **Francesca Blythe** explain what organisations have to look out for.

The EU's General Data Protection Regulation (GDPR) was adopted by the European Parliament on 14 April 2016. The final step for formal adoption was publication of the GDPR in the Official Journal of the EU on 4 May which means that the starting date for the two-year implementation period will be 24 May 2016. Companies and data protection authorities (DPAs) will then have just 24 months from this date to implement the new requirements under the GDPR.

The GDPR is intended to create a single harmonised data protection law across the EU. However, in the text adopted by the Parliament, there are approximately 30 instances where Member States have been given the ability to legislate at a national level. This will result in national law differences in Member States and mean that businesses – even after the GDPR becomes law in 2018 – will still need to consider data protection laws in different parts of the European Union. While some DPAs will probably take a strict approach, the UK's Information Commissioner is likely to be more commercial in its approach and implement derogations which will likely assist businesses in their compliance with the GDPR. Summarised below are some of the key provisions in the GDPR which contain national law derogations.

Legal grounds for processing

In order to process personal data lawfully the processing must be based on one or more of the conditions set out in Article 6(1) of the GDPR. The conditions specified are largely the same as those in the current EU Data Protection Directive 95/46/EC (Directive) and include, for example, where the processing is based on the legitimate interests of the controller. However, Article 6(2) of the GDPR permits Member States to introduce additional requirements or specifications to ensure fair and lawful processing in relation to:

1. where the processing is necessary for compliance with a legal obligation (Article 6(1)(c)); or
2. where the processing is necessary for the performance of a task carried out in the public interest (Article 6(1)(e)).

As under the Directive, an additional legal condition such as, explicit consent, must be satisfied when processing sensitive personal data, such as data on health, trade union membership and ethnicity. However, Article 9(2)(a) of the GDPR states that even if a data subject explicitly consents, Member State law may still prohibit the processing of sensitive personal data despite consent. In addition, pursuant to Article 9(4) in relation to the processing of genetic data, biometric data or health data, Member States may introduce further conditions, including limitations, on how such data can be processed.

The GDPR also limits the way in which personal data relating to criminal convictions and offences are processed. Such personal data may be processed only under the control of an official authority (e.g. the police), or where authorised under Member State law. In both instances, appropriate safeguards to protect the rights and freedoms of data subjects must be in place.

These provisions mean that companies processing sensitive personal data, for example, those in financial services and healthcare sectors, will need to continue to check the position in each relevant Member State.

Children's data

The GDPR further introduces specific requirements for the processing of the personal data of a child. The GDPR requires that such processing in relation to the offering of information society services (e.g. through a website or social media platform) directly to children under 16 years old, or 13 years if permitted under EU Member State national law, requires the consent from the child's parent or legal guardian. This derogation, allowing different age requirements across EU Member States, could pose considerable challenges for businesses which offer ecommerce or social media services, as the age at which a person is considered a child is unlikely to be consistent. We understand, for example, that the UK has indicated it will be lowering the age limit to 13 years.

Fines and sanctions

The powers afforded to DPAs are significant including powers to suspend data transfers to recipients in non-EU countries and impose temporary or permanent bans on the processing of personal data. Pursuant to Article 58(6), Member States are also able to create laws that grant additional "corrective" powers to their DPAs over and above those explicitly granted to DPAs under the GDPR.

DPAs also have the power to impose fines for non-compliance of up to the greater of 4% of annual worldwide turnover or €20 million. Article 84(2) permits Member States to impose their own rules on the penalties applicable to infringements of the GDPR. These derogations will certainly lead to variations in enforcement powers for different DPAs and inconsistent application of fines in different Member States as currently exists under the Directive.

Accountability

Core to the GDPR are the enhanced accountability principles which require businesses to adopt and implement policies and procedures to demonstrate compliance with the data protection requirements. This in part demonstrates the shift away from the more bureaucratic approach to compliance adopted under the Directive. For example, the removal of the requirement to notify DPAs of processing

activities other than in limited circumstances (e.g. where required by Member State law in relation to processing by a controller for the performance of a task carried out in the public interest).

A key way to demonstrate accountability is the requirement for controllers to carry out data protection impact assessments where new technologies are being used or where processing may pose high risks to individuals. In addition, pursuant to Article 35(1) processors may be required to carry out such assessments prior to conducting their processing activities, if required to do so by Member State law, even where a data protection impact assessment has already been undertaken by a controller.

Controllers and processors are also required to appoint a data protection officer (DPO) if they are engaged in:

1. the regular or systematic monitoring of data subjects on a large scale;
2. the processing of sensitive personal data on a large scale; or
3. the processing is carried out by a public authority. In addition, importantly a DPO may also be required pursuant to Article 37(4) if mandated under national Member State law.

So again in relation to the core concept of accountability the principle of a harmonised EU data protection law under the GDPR appears somewhat undermined by national law derogations.

Processors

Under the GDPR, processors will, for the first time, have specific statutory obligations that they must comply with when processing personal data. These include a requirement only to process personal data on the instructions of the controller, unless required under Member State law, in which case the processor must inform the controller of these legal requirements in advance. A further derogation specific to processors provides that where the controller requests the deletion of data at the end of the provision of services, this is subject to where the processor is required to store the data pursuant to Member State law.

So companies that act as data processors, such as cloud providers, will also need to continue to be aware of national law requirements in different EU Member States.

Data Subject rights

The GDPR introduces a number of new rights for data subjects which are subject to a blanket derogation in Article 23(1) which permits Member State law to restrict the scope of these rights where such a restriction is "necessary and proportionate in a democratic society". Such a broad general derogation and further specific derogations for specific rights as described below, will lead to uncertainty as to how these rights will be applied across the EU.

One of the more talked about new rights is the statutory right for data subjects to have their personal data erased without undue delay where, for example, the consent for the processing is withdrawn and there is no other legal basis for the processing, or, in order to comply with a legal obligation in a Member State law to which the controller is subject. However, the right to erasure will not apply where the processing is necessary to comply with a legal obligation in that Member State.

Article 14 sets out the information to be provided to data subjects where the personal data have been obtained other than from the data subject. These information requirements are much more extensive than under the Directive and should be provided within one month of the receipt of the data, at the time of communication with the data subject or when the data is first disclosed to a third party. However, this information does not need to be provided where, for example, it is a Member State legal requirement to obtain or disclose such data or the data must remain confidential pursuant to an obligation of secrecy regulated by Member State law.

The GDPR also introduces new restrictions in respect of profiling, with data subjects having a right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects him or her. This right is subject to a limited number of exemptions including, for example, where the processing is authorised by EU or national Member State law to which the controller is subject (Article 22 (2)(b)).

International data transfers

The GDPR maintains the current restrictions under the Directive on transfers of personal data from the EU to a third country not deemed to have adequate levels of protection by the Commission. However, pursuant to Article 49(5), in the absence of an adequacy decision, Member State law may, for important reasons of public interest, set limits to the transfer of specific categories of personal data to a third country or international organisation, providing the Member State notifies such provisions to the Commission. Once again, such national law limits and derogations on international transfers will require international companies to continue to check the national law position in different Member States.

Further derogations

Chapter IX of the GDPR sets out requirements for specific processing situations including, for example, in relation to employee data (which will impact nearly all companies) and processing for scientific research purposes (which will impact companies in the life sciences industry). In each of these situations as described further below, the GDPR provides that Member States can provide specific exemptions, derogations, conditions or rules for the processing of these types of data, giving Member States more control over the way in which such data is processed and further undermining the principle of a single, harmonised EU data protection law.

Article 88 sets out the provisions in relation to processing in the employment context. Member States can implement (either by law or by collective agreements) specific rules in respect of the processing of employees' personal data for all key purposes from recruitment through to termination of the employment relationship. Member States must notify the Commission of any such specific laws established pursuant to Article 88 without delay and at least by 2020. Any subsequent amendment affecting such laws must also be notified. The derogations in this Article 88 mean that employers of multi-national companies will likely need to comply

with a myriad of inconsistent employment laws impacting the use of employee data across Europe.

Article 89(2) provides that where personal data are processed for statistical, scientific or historical research purposes, Member States may provide derogations from certain data subject rights (including, the rights to access, rectification, restriction and objection) where such rights are "likely to render impossible or seriously impair the achievement of the specific purposes" and the derogation is necessary to meet those requirements. For companies in the life sciences industry this Article may cause concern where, for example a company is running a clinical trial across multiple Member States and the position as to compliance with these data subject rights may vary.

Additional broad derogations are set out in Article 23(1) which permits Member States to implement legislative restrictions in respect of the data protection principles and the data subject rights provided that any such restriction "respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society..." The measure must safeguard one of a limited number of factors including, for example:

4. national security;
5. the prevention, investigation or detection of crime; or
6. the protection of the data subject or the rights and freedoms of others.

Conclusion

In conclusion, the numerous derogations that exist in the GDPR undermine the core principle of the GDPR – to create a single EU-wide law on data protection to increase legal certainty for all stakeholders. The GDPR was also intended to reduce the cost of the administrative burden resulting from legal fragmentation. However, the large number of derogations and their potential broad scope is likely to result in many international companies having to continue to deal with national data protection law variations across numerous Member States to ensure compliance with the varying EU data protection requirements.

AUTHORS

William Long is a Partner and Francesca Blythe an Associate at Sidley Austin LLP.
Emails: wlong@sidley.com
fblythe@sidley.com