Material and territorial scope

At a glance

- As compared to Directive 95/46/EC (the "Data Protection Directive") which it replaces, the GDPR seeks to extend the reach of EU data protection law.
  - An EU based data controller and processor falls into its scope where personal data is processed *"in the context of its activities"* - a broadly interpreted test.
  - Where no EU presence exists, the GDPR will still apply whenever: (1) an EU resident's personal data is processed in connection with goods/services offered to him/her; or (2) the behaviour of individuals within the EU is *"monitored"*.
- Despite being a Regulation, the GDPR allows Member States to legislate in many areas. This will challenge the GDPR's aim of consistency, including employee data processing.
- The GDPR does not apply to certain activities – including processing covered by the Law Enforcement Agencies ("LEA") Directive, for national security purposes and processing carried out by individuals purely for personal/ household activities.
- The GDPR will take effect on 25 May 2018.

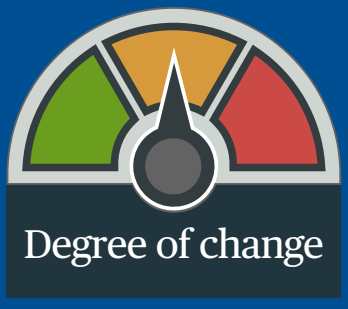
To do list

☐ Organisations without an EU presence, but who target or monitor EU individuals, should:

- understand the impact of the GDPR; and
- determine an approach to compliance.

☐ Organisations working in areas where *"special"/sectoral* rules are common, should:

- assess if they require specific Member State laws and advocate these if necessary; and
- keep a watching brief on such laws being promulgated in ways which may be unhelpful for them.



Territorial scope

EU "established" controllers or processors

The GDPR will apply to organisations which have EU *"establishments"*, where personal data are processed *"in the context of the activities"* of such an establishment.

If this test is met, the GDPR applies irrespective of whether the actual data processing takes place in the EU or not.

"Establishment" was considered by the Court of Justice of the European Union ("CJEU") in the 2015 case of *Weltimmo v NAIH* (C-230/14). This confirmed that establishment is a *"broad"* and *"flexible"* phrase that should not hinge on legal form. An organisation may be *"established"* where it exercises *"any real and effective activity – even a minimal one"* – through *"stable arrangements"* in the EU. The presence of a single representative may be sufficient. In that case, Weltimmo was considered to be established in Hungary as a result of the use of a website in Hungarian which advertised Hungarian properties (which meant that, as a consequence, it was considered *"mainly or entirely directed at that Member State"*), use of a local agent (who was responsible for local debt collection and acted as a representative in administrative and judicial proceedings), and use of a Hungarian postal address and bank account for business purposes – notwithstanding that Weltimmo was incorporated in Slovakia.

Organisations which have EU sales offices, which promote or sell advertising or marketing targeting EU residents will likely be subject to the GDPR – since the associated processing of personal data is considered to be *"inextricably linked"* to and thus carried out *"in the context of the activities of"* those EU establishments *(Google Spain SL, Google Inc. v AEPD, Mario Costeja González* (C-131/12)).

Non-EU "established" organisations who target or monitor EU data subjects

Non-EU established organisations will be subject to the GDPR where they process personal data about EU data subjects in connection with:

- the *"offering of goods or services"* (payment is not required); or
- *"monitoring"* their behaviour within the EU.

For offering of goods and services (but not monitoring), mere accessibility of a site from within the EU is not sufficient. It must be apparent that the organisation *"envisages"* that activities will be directed to EU data subjects.

Contact addresses accessible from the EU and the use of a language used in the controller's own country are also not sufficient. However, the use of an EU language/currency, the ability to place orders in that other language and references to EU users or customers will be relevant.

The CJEU has examined when an activity (such as offering goods and services) will be considered *"directed to"* EU Member States in a separate context (i.e. under the "Brussels 1" Regulation (44/2001/EC) governing *"jurisdiction…in civil and commercial matters"*). Its comments are likely to aid interpretation under this similar aspect of the GDPR. In addition to the considerations mentioned above, the CJEU notes that an intention to target EU customers may be illustrated by: (1) *"patent"* evidence, such as the payment of money to a search engine to facilitate access by those within a Member State or where targeted Member States are designated by name; and (2) other factors – possibly in combination with each other – including the *"international nature"* of the relevant activity (e.g. certain tourist activities), mentions of telephone numbers with an international code, use of a top-level domain name other than that of the state in which the trader is established (such as .de or .eu), the description of *"itineraries…from Member States to the place where the service is provided"* and mentions of an *"international clientele composed of customers domiciled in various Member States"*. This list is *not exhaustive* and the question should be determined on a case-by-case basis *(Pammer v Reederei Karl Schlüter GmbH & Co and Hotel Alpenhof v Heller* (Joined cases (C-585/08) and (C-144/09)).

It is not clear whether non-EU organisations offering goods and services to EU businesses (as opposed to individuals) will fall within the scope of the "offering goods and services" test in Article 3(2)(a).

"Monitoring" specifically includes the tracking of individuals online to create profiles, including where this is used to take decisions to analyse/predict personal preferences, behaviours and attitudes.

Organisations subject to the GDPR's *long-arm* jurisdictional reach must appoint an EU-based representative.

Under the Data Protection Directive, organisations targeting EU data subjects only had to comply with EU rules if they also made use of *"equipment"* in the EU to process personal data. This led national supervisory authorities, who were seeking to assert jurisdiction, to develop arguments that the placing of cookies, or requesting users to fill in forms, would amount to the use of *"equipment"* in the EU. It will now be easier to demonstrate that EU law applies. (Although, where organisations have no EU presence, enforcement may be just as difficult as before).

Where EU member state law applies by virtue of public international law

Recital 25 gives the example of a diplomatic mission or consular position.

Exclusions

Certain activities fall entirely outside the GDPR's scope (listed below).

In addition, the GDPR acknowledges that data protection rights are not absolute and must be balanced (proportionately) with other rights – including the *"freedom to conduct a business"*. (For the ability of Member States to introduce exemptions, see section on derogations and special conditions). As the GDPR toughens up many areas of data protection, introducing more new sticks than regulatory carrots, businesses may find it helpful to bookmark this statement in Recital 4 in case of future need.

The GDPR does not apply to the processing of personal data (these general exemptions are very similar to the equivalent provisions included in the Data Protection Directive):

- in respect of activities which fall outside the scope of EU law (e.g. activities concerning national security);
- in relation to the EU's common foreign and security policy;
- by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences and associated matters (i.e. where the Law Enforcement Agencies ("LEA") Directive[1], which was adopted as EU 2016/618 on 26 April 2016 now applies);
- by EU institutions, where Regulation 45/2001/EC will continue to apply instead of the GDPR. This Regulation is to be updated to ensure consistency with the GDPR; and
- by a natural person as part of a *"purely personal or household activity"*. This covers correspondence and the holding of address books – but it also now covers social networking and online activities undertaken for social and domestic purposes. It represents a possible widening of the exemption from the principles set out in *Bodil Lindqvist* (C-101/01), before the advent of social media. In this case, the CJEU noted that sharing data with the Internet at large *"so that those data are made accessible to an indefinite number of people"* could not fall within this exemption, which it stated should be limited to activities *"carried out in the course of the private or family life of individuals"*. Note also that the GDPR will remain applicable to controllers and processors who *"provide the means for processing"* which falls within this exemption.

The GDPR is stated to be *"without prejudice"* to the rules in the E-commerce Directive (2000/31/EC), in particular to those concerning the liability of *"intermediary service providers"* (and which purport to limit their exposure to pecuniary and criminal liability where they merely host, cache or act as a *"mere conduit"*). The relationship with the E-commerce Directive is not straightforward – as that Directive states that issues relating to the processing of personal data are excluded from its scope and *"solely governed"* by relevant data protection legislation. The two can be read consistently if one assumes that the liability of ISPs for the actions of users will be determined by the E-commerce Directive, but that other matters (such as obligations to erase or rectify data, or obligations on an ISP concerning its own uses of personal data) will be governed by the GDPR. However, the point is not clear.

Regulation versus national law

As a Regulation, the GDPR will be directly effective in Member States without the need for implementing legislation.

However, on numerous occasions, the GDPR does allow Member States to legislate on data protection matters. This includes occasions where the processing of personal data is required to comply with a legal obligation, relates to a public interest task or is carried out by a body with official authority. Numerous articles also state that their provisions may be further specified or restricted by Member State law. Processing of employee data is another significant area where Member States may take divergent approaches.

Organisations working in sectors where *special rules* often apply (e.g. health and financial services) should: (1) consider if they would benefit from such *"special rules"* which would particularise or liberalise the GDPR; and (2) advocate these accordingly. They should also watch for Member States seeking to introduce *"special rules"* which may prove restrictive or inconsistent across Member States.

Where can I find this?

Material Scope	*Article 2*	*Recitals 15-21*
Territorial Scope	*Article 3*	*Recitals 22-25*

[1] Full title: Directive *"on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data."*