Meritas Data Protection & Privacy Law

GDPR: New territorial scope, one stop shop and consistency mechanisms

LYDIAN

MERITAS
LAW FIRMS WORLDWIDE

One of the undeniable highlights of the new General Data Protection Regulation (***GDPR***), which will come into force on 25 May 2018, is its extended territorial scope. The new geographical reach does not only come as a reaction to a changing reality of a globalised world, but also follows a trend which is already apparent in recent case law under the current Data Protection Directive and which is to extend the extraterritorial reach of said Directive.

1. THE EXTENDED TERRITORIAL SCOPE

1.1. Organisations established in the EU

The GDPR applies to the processing of personal data by controllers and processors having an '*establishment*' in the EU, where such processing takes place "*in the context of the activities*" of such an establishment, irrespective of whether the processing takes place inside or outside the EU.

'*Establishment*' within the meaning of the Regulation implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not a determining factor.

It is not entirely clear whether the CJEU case law under the Data Protection Directive, as reflected in *Weltimmo* (C-230/14) and *Google Spain* (C-131/12), and which both gave a very broad interpretation to the term '*establishment*', will be of further relevance once the GDPR comes into force. More precisely, in *Weltimmo*, the Court ruled that "*any real and effective activity – even a minimal one*" is sufficient to trigger application of the Data Protection Directive. In *Weltimmo*, the CJEU concluded that

Weltimmo, a Slovakian company, was established in Hungary on the basis of (i) the use of a website in Hungarian listing Hungararial real estate and thus "*mainly or entirely directed at that Member State*", (ii) the use of a local agent and (iii) the use of a Hungarian postal address and bank account. In *Google Spain*, the CJEU decided that the US company Google Inc. was established in the EU due to the fact that the processing of personal data was "*inextricably linked*" to the activities of its Spanish subsidiary.

1.2. Organisations not established in the EU

Under the Data protection Directive, data controllers established outside of the EU but using equipment in the EU fall under EU data protection regulation. Apart from traditional forms of equipment, case law extended this to also include servers, employees or representatives.
Under the GDPR, non-EU established organisations – controllers and processors – will be subject to the GDPR, where the processing activities are related to:

(a) the offering of goods or services to data subjects in the EU; or

(b) the monitoring of the behaviour of data subjects in the EU, to the extent such behaviour takes place within the EU.

Clarification on whether or not citizens within the EU are being offered goods and services, is being provided in Recital 23 of the GDPR, which reflects the case law of the CJEU, and more precisely the principles laid down in *Weltimmo*. As such, the basic criterion is whether or not the controller or

processor outside of the EU envisages offering services to data subjects in one or more Member States of the EU. Such might be the case if a company uses a language or a currency used in one or more Member States, with the possibility of ordering goods and services in that language, or in case customers or users who are in the EU are being mentioned.

The monitoring of behaviour relates to whether individuals are tracked on the internet, including potential subsequent use of personal data processing techniques which consist of profiling of an individual, particularly in order to take decisions concerning her/him for analysing or predicting her/his personal preferences, behaviours or attitudes. In this regard, it will be interesting to see how strict these provisions will be interpreted, especially with regard to for example IP addresses, incidental collection of data by non-EU controllers or the use of cookies.

1.3. Public international law

Finally, the GDPR applies to the processing of personal data by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law. It should be noted that this is limited to controllers.

2. EXTRA-TERRITORIAL APPLICATION TO PROCESSORS

Where non-EU established processors *directly* offer goods or services to individuals in the EU (e.g., cloud services) or *directly* monitor the behaviour of individuals in the EU, the GDPR will apply directly to the

processing of personal data related thereto and the non-EU established processors will be subject to the GDPR.

It is however far less clear to what extent this reasoning will apply when a non-EU processor is delivering services to a controller or processor based in the EU. Arguably, the non EU processor might be considered to be processing personal data "*in the context of the activities of an establishment of a controller or a processor in the EU*".

Another hypothesis which reflects the potentially broad scope of the GDPR is when a non-EU entity provides services to a non-EU established controller or processor which in turn offers goods or services to individuals in the EU or monitors the behaviour of individuals in the EU. Whether or not such services will be qualified as "*related to*" offering goods or services or monitoring of the behaviour of individuals, will need to be clarified in the coming months and years.

3. APPOINTMENT OF A REPRESENTATIVE

Once the GDPR applies to a non-EU established controller or processor, such controller or processor will be under an obligation to appoint a representative based in the EU. Such representative must be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.
The representative must be mandated (in writing) by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and

data subjects, on all issues related to processing, for the purposes of ensuring compliance with the GDPR.

It is unclear whether the representative is merely a single point-of-contact within the EU for supervisory authorities and data subjects or whether it can also be held liable for breach of the GDPR. Recital 80 of the GDPR states that the designated representative "*should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance*" and "*should be subject to enforcement proceedings in the event of non-compliance by the controller or processor*". Pursuant to Article 27(5) GDPR, the designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves. It is unclear whether this also means that representatives can be the subject of fines, penalties and other sanctions imposed by supervisory authorities or liability vis-à-vis data subjects. Chapter III (*Remedies, liability and penalties*) of the GDPR does contain any reference to the representatives designated pursuant to Article 27 of the GDPR.

4. ONE STOP SHOP PRINCIPLE

In order to ensure correct application of the GDPR, effectiveness in supervision and a reduction of the administrative burden, the Commission's initial proposals allowed a '*single supervisory authority*' (SSA) to take full responsibility for the EU-wide data processing obligations of the controllers which had their main establishment within their territory. For fear of forum shopping by controllers and processors with

broad processing activities, and because of the difficulties the data subjects might encounter when exercising their rights, this proposal did not make it to the GDPR.

Currently in the GDPR, in case of cross-border processing, there will be one supervisory authority in charge of leading the supervision. Nonetheless, there are several mechanisms which nuance and moderate the upper hand of the lead supervisory authority.

4.1. Lead supervisory authority

In contrast to the Directive, the GDPR has introduced a system in which one supervisory authority takes the lead in the supervision of controllers or processors carrying out cross-border processing operations. 'Cross-border processing' means either

(i) where the controller or processor is established in more than one Member State, the processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the EU; or

(ii) where the controller or processor is established in a single Member State, the processing of personal data which takes place in the context of the activities of such single establishment of a controller or processor in the EU but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

The 'lead supervisory authority' is the supervisory authority of the main establishment or of the single establishment of the controller or processor.

In respect of a *controller* with establishments in more than one Member State, 'main establishment' means the place of its central administration in the EU, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the EU and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment.

In respect of a *processor* with establishments in more than one Member State, 'main establishment' means the place of its central administration in the EU, or, if the processor has no central administration in the EU, the establishment of the processor in the EU where the main processing activities in the context of the activities of an establishment of the processor take place.

4.2. Other supervisory authorities

Even where a lead supervisory authority is competent for 'cross-border processing', other supervisory authorities (the so-called 'concerned supervisory authorities') will remain competent to handle complaints lodged with it or a possible infringement of the GDPR, if the subject matter (i) relates only to an establishment in its Member State or (ii) substantially affects data subjects only in its Member State.

In the event a concerned supervisory authority would wish to investigate such complaint or infringement, it should notify the lead supervisory authority, which in return has a period of three weeks to determine whether it would want to intervene and apply the cooperation procedure (see below).

Even if the cooperation procedure is triggered, the concerned supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority must "*take utmost account of*" that draft when preparing the draft decision under the cooperation procedure.
In case the lead supervisory authority does not wish to intervene, the local authority handles the case using, where necessary, the mutual assistance and joint operations powers.

5. COOPERATION PROCEDURE

If the lead supervisory authority wishes to intervene and thus apply the cooperation procedure, the latter will in the conduct of its task have the obligation to cooperate with other concerned supervisory authorities, with the purpose of reaching a consensus on the decisions which are to be taken. In this regard, the lead supervisory authority has to provide the concerned supervisory authority with information, and has to submit drafts of its decisions to the concerned supervisory authority, which has four weeks to raise any objections. Furthermore, the lead supervisory authority can also request the concerned supervisory authority's assistance and can conduct joint operations within the concerned supervisory authority's Member State.
In case the lead supervisory authority does not intend to act in accordance with the views of a concerned supervisory authority, the latter has the possibility to trigger the consistency mechanism (see below).

6. MUTUAL ASSISTANCE AND JOINT OPERATIONS

In any case, supervisory authorities are required to provide each other assistance in the form of information sharing or by carrying out prior authorisations and consultations, inspections and

investigations. **THE** requested supervisory authority may not refuse such requests unless it is not competent for the subject-matter or for measures it is requested to execute or when compliance with the request would infringe the GDPR or EU or Member State law. Once competent, requests must be granted without undue delay, and in any event within one month.

Furthermore, supervisory authorities can conduct joint investigations and enforcement operations. Supervisory authorities have conducted joint investigations under existing law too, so the GDPR will in practice only develop and strengthen these arrangements.

A supervisory authority will have the right to be involved in enforcement operations if a controller has an establishment in its territory, or if a significant number of data subjects are likely going to be affected. If national law permits this, a host supervisory authority can give formal investigatory powers to seconded staff.

7. CONSISTENCY MECHANISM

Against the potential danger of diverging views by the various supervisory authorities on the principles and obligations laid down in the GDPR, the European Data Protection Board (EDPB) will most likely play a crucial role.

The EDPB will replace the current Article 29 Working Party and will consist of the heads of the supervisory authorities, as well as the European Data Protection Supervisor (EDPS).

Aiming at the consistent application of the GDPR throughout the EU, the EDPB will be active as an independent body with its own legal responsibility. The task of the EDPB is twofold: on the one hand it will provide guidance on data protection, where it will issue opinions; on the other hand it will fulfil a role as a dispute resolution mechanism, where it will issue binding decisions.

7.1. Opinions of the EDPB

As such, the EDPB will issue an opinion where a competent supervisory authority (i) intends to adopt a list of the processing operations subject to the requirement for a data protection impact assessment, (ii) it concerns a matter regarding a draft code of conduct contributing to the proper application of the GDPR, (iii) the draft decisions aims at accrediting a certification body, (iv-v) when it aims at determining or authorising standard data protection clauses in case of data transfers to third countries or finally (vi) when the draft decision aims at approving binding corporate rules in the light of data transfers to third countries.

Furthermore, any supervisory authority, the Chair of the EDPB or the Commission may request that any matter of general application or producing effects in more than one Member State be examined by the EDPB.

7.2. Dispute resolution mechanism

The EDPB will issue a binding decision in case (i) supervisory authorities do not agree on the draft of measures which are to be adopted under the cooperation procedure or (ii) there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment or finally (iii) when the opinion of the EDPB has not been requested where it should have been or when this opinion is not followed by the competent supervisory authorities.

In all these cases, the EDPB takes a binding decision on the basis of a two-thirds majority vote. If there is no such majority, then after a delay, a simple majority will suffice. The supervisory authorities

involved are bound to comply and formal decisions have to be issued in compliance with the EDPB decision.

8. URGENCY PROCEDURE

Notwithstanding the activation of the consistency mechanism, the lead supervisory authority remains competent to derogate from the consistency mechanism and take urgent provisional measures on its territory in order to protect the rights and freedoms of its data subjects. There provisional measures shall however not exceed a period of three months and will have to be notified to the EDPB and the Commission.

Furthermore, where a supervisory authority has already taken urgent measures on its own territory and considers that final decisions need urgently be adopted, the EDPB will adopt an urgent opinion or decision within two weeks with a simple majority of the members of the EDPB. The same is possible at the request of any supervisory authority in case a competent supervisory has failed to take appropriate measures in order to protect the rights and freedoms of data subjects.

Bastiaan Bruyndonckx
Partner, Head of ICT Team
Lydian, Belgium
bastiaan.bruyndonckx@lydian.be

LYDIAN

MERITAS
LAW FIRMS WORLDWIDE

About the Author

Bastiaan Bruyndonckx is a Partner in Lydian's Commercial & Litigation practice where he heads the Information and Communication Technology (ICT) practice and the Information Governance & Data Protection (Privacy) practice. He specializes in all aspects of Information and Communication Technology law, with a particular focus on information governance, technology procurement and outsourcing contracts, electronic communications and e-commerce. He advises companies in a broad range of industry sectors on information governance and data protection (privacy) matters. Bastiaan is a member of the International Association of Privacy Professionals (IAPP).

www.lydian.be