Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 2 >>> FEBRUARY 2016

Data Processors

European Union

The EU General Data Protection Regulation: A Brave New World for Processors

By Victoria Hordern

Significant changes are afoot for processors. With the text of the European Union General Data Protection Regulation (GDPR) now published, processors will need to begin to acclimatise to the new regime under the GDPR . This article examines the key changes and what the probable implications will be.

Victoria Hordern is a senior associate at Hogan Lovells, London.

For non-EU privacy professionals, it can be a little baffling that EU law distinguishes between organisations that handle personal information labelling them either controllers or processors. Neither of the documents from the early 1980s that influenced the shape of EU data protection law—the Organisation for Economic Cooperation and Development Guidelines and the Council of Europe Convention 108—mentioned the concept of processors. Though the EU had an opportunity to retire the processor label (or at least recognise that there may be technology platforms which operate neither as a controller or processor) as part of their recent review of the EU data protection framework, this has not taken place.

Origin of Processors

It was the 1995 EU Data Protection Directive (Directive) that introduced the concept of a processor but without any explanation provided in the Directive. However, earlier versions of the draft Directive proposed by the Commission indicate that the concept of

a processor was necessary to avoid situations where the use of a third party by a controller reduces the level of protection for the individual.

The Directive states that a processor is an entity or person that processes personal data on behalf of a controller, must keep the personal data confidential and secure and only use it in accordance with the instructions of a controller. Any responsibility for compliance with data protection principles, any liability or sanctions are laid at the door of the controller. That's not to say that processors are always beyond the reach of EU data protection authorities (DPAs). Controller's can place contractual obligations on processors requiring them to comply with investigations and enquiries made by DPAs in relation to the controller's personal data. But essentially any liability for processors is set out in the contract between controllers and processors.

The Changing Environment

So why does the new GDPR extend direct application of the law to processors and make them subject to fines from DPAs? In a 2009 paper commenting on the EU data protection reforms, the Article 29 Working Party (Working Party) indicated that the roles of controllers and processors were often blurred and that the DPAs should have the power to impose financial sanctions on both controllers and processors[1] Yet in a 2010 Opinion looking at the roles of controllers and processors, the Working Party did not specifically recommend that processors be subject to direct legal obligations.[2] The Opinion confirmed that, although technological advancements had made processing environments increasingly complex, it did not find any reason to think that the current distinction between the two roles was no longer relevant and workable. In the Working Party's view, it is about the need to allocate responsibility between the parties in such a way that compliance with data protection rules is sufficiently ensured in practice.

Suffice to say that the General Data Protection Regulation still places the lion's share of compliance responsibilities on controllers.

The latest draft of the GDPR (which is likely to be the final text) does not provide any detailed explanation as to why processors will be subject to direct obligations under the new law. However, in a number of places it is clear that part of the motivation is to ensure individuals have legally enforceable rights. Suffice to say that the GDPR still places the lion's share of compliance responsibilities on controllers. For instance, it is the controller who is responsible for and is required to demonstrate compliance with the principles relating to personal data processing. Likewise it is the controller's responsibility to provide effective information to the individuals about the processing of their personal data and it is the controller who must respond when individuals exercise their rights to access their data.

So What Are the Changes That Affect Processors Under the GDPR?

1. **Data protection law will apply directly**. The GDPR will apply to processing of personal data carried out by a processor established in the EU even if the actual processing takes place outside the EU. So a cloud provider in Germany who processes personal data for customers in the context of activities provided by the German business is caught whether the data is hosted on servers in Germany or India. Moreover, recent decisions from the Court of Justice of the EU have underlined that the concept of "establishment" is interpreted broadly[3] Consequently, a minimal amount of economic activity, such as a U.S.-based company using a single sales representative operating in an EU country, can be sufficient to trigger the establishment requirement and hence application of EU data protection law.

The law also applies to a processor not established in the EU where it offers goods or services to EU residents or monitors the behaviour of EU residents and consequently processes their personal data. So a U.S. ad network provider with U.S. corporate customers who wish to target ads and profile EU residents will be caught even though it has no physical presence in the EU (and of course the U.S. corporate customers are also caught). In such circumstances, the non-EU processor is required to designate an EU representative (unless the data processing is occasional and is not a high risk to individuals).

This is a significant change. Processors are not currently subject to direct obligations under the Directive (though there may be limited obligations chiefly around registration in certain Member States). In particular, many non-EU companies who have targeted EU consumers but operated on the basis that EU law does not apply to them will have to adapt to the new regime. Of course, one of the ensuing dilemmas for European DPAs and courts will be how to enforce the rules of the GDPR on processors based in, for example, the U.S., Russia and India but with no physical presence in the EU.

2. **Relationships with controllers will be more strictly regulated**. The existing provisions in the Directive on appointing a processor are reflected in the GDPR e.g. implementing appropriate technical and organisational security measures. But there are new requirements such as the restriction on processors engaging another processor without the consent of the controller. This can be a general written consent provided by the controller but, in such cases, the controller has the right to object to the new processor. The processor is required to impose the same data protection obligations on the new proces-

[1] Article 29 Data Protection Working Party, "The Future of Privacy, Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data," 1 Dec. 2009, WP 168, paragraph 90.

[2] Opinion 1/2010 on the concepts of "controller" and "processor," 16 Feb. 2010, WP 169 .

[3] *See Weltimmo sro v Nemzeti Adatvédelmi és Információszabadság Hatóság* C-230/14 (1 Oct. 2015) and *Google Spain SL and Google Inc v Agencia Española de Protección de Datos and Mario Costeja González* C-131/12 (13 May 2014).

   ISSN 1473-3579

sor and the initial processor remains fully liable for the performance of the new processor.

Additionally, the contract with the controller must provide more detail about the processing the processor is engaged in: the subject-matter, duration, nature and purpose of the processing, the type of personal data and categories of individuals and obligations and rights of the controller. The processor must also comply with a controller's instructions on data transfers outside the EU, ensure that processor personnel are subject to confidentiality, help the controller respond to requests from individuals, assist the controller with data security, data breaches, privacy impact assessments and when consulting with the DPA. Furthermore, the processor must delete or return all data to the controller at the end of data processing services, make information available to the controller to demonstrate the processor's compliance and permit audits.

Processors will be required to appoint a data protection officer where their core processing activities involve on a large scale either (i) regular and systematic monitoring of individuals or (ii) processing of sensitive or criminal data.

3. **Processors must demonstrate accountability**. A processor must maintain a record of all of its data processing activities (apart from if it employs fewer than 250 people and is not engaged in high risk processing). This includes details such as categories of processing and data transfers to non-EU countries. The processor is required to provide the records to the DPA if requested. This obligation will require processors such as cloud service providers to document all their processing activities for customers even if their services do not effectively "touch" customer data.

Processors will also be required to appoint a data protection officer (DPO) where their core processing activities involve on a large scale either (i) regular and systematic monitoring of individuals or (ii) processing of sensitive or criminal data. It is at least possible that monitoring technologies such as data loss prevention offered by cloud providers will be deemed regular and systematic monitoring of individuals on a large scale and thus trigger the requirement for a DPO. It is the role of the DPO to advise the processor about compliance with the GDPR and monitor compliance, as well as acting as the contact point for the DPA.

Processors may choose to adhere to a code of conduct or certification scheme that is recognised under the GDPR. Compliance with the code or scheme can help to demonstrate that the processor is implementing appropriate security measures and is complying with its GDPR obligations. But adherence to a code or scheme brings with it greater scrutiny and, if there is a failure, the prospect of being publicly suspended or excluded from the code or scheme.

4. **Both parties are directly responsible for data security**. The headline requirement under the GDPR to keep personal data secure is expressed as an obligation on both controllers and processors. There is a positive obligation to consider pseudonymisation and encryption, ensure on-going confidentiality, integrity, availability and resilience of systems and services, restore access to data, and operate a process to regularly test, assess and evaluate the effectiveness of security measures. While it is the controller's obligation to respond in full to data security breaches, the processor must notify the controller without undue delay after becoming aware of a breach and assist the controller to comply with data security breach obligations.

5. **Rules on data transfers and disclosures**. Processors alongside controllers are responsible for compliance with the data transfer rules and can make data transfers to non-adequate countries where they have adduced appropriate safeguards and secured enforceable rights and effective legal remedies for individuals. Binding corporate rules for processors is officially recognised as a solution under the GDPR.

The GDPR acknowledges that a processor may itself be subject to direct legal requirements to process the personal data it holds on behalf of a controller but these actions are only permitted where the processor is subject to EU or Member State law i.e. not where the processor is required under non-EU law. If a processor receives a request from a non-EU court, tribunal or administrative authority to disclose data held in the EU (and therefore make a data transfer) and it cannot rely on another ground for transfers, this request is only recognised under the GDPR if based on an international agreement (such as a mutual legal assistance treaty (MLAT)) in force between the non-EU country and the EU or Member State.

The role of Data Protection Authorities will loom much larger over processors under the General Data Protection Regulation. Not only will processors be under a direct obligation to co-operate with a DPA, but a DPA will have investigatory powers over processors.

The position under the GDPR on this point is unsurprising in view of the discussions within the EU since the Snowden revelations around transatlantic data transfers and access to data by government agencies. However, it still leaves processors holding data in the EU in an unenviable position if they receive an urgent request from a non-EU government agency for access to that data given the need to comply with the rules under the GDPR and rely on a MLAT which can be a lengthy process.

6. **Processors will be subject to greater regulatory and judicial exposure**. The role of DPAs will loom much

larger over processors under the GDPR. Not only will processors be under a direct obligation to co-operate with a DPA, but a DPA will have investigatory powers over processors, can obtain access to all the personal data a processor holds, can access processor premises, issue warnings, order compliance, ban processing and ultimately issue fines (up to 4 percent of total worldwide annual turnover). However, it is important to note that the circumstances under which a processor could receive the highest fine are narrower than for controllers.

Of huge significance is the right that individuals will have to seek a judicial remedy and claim compensation against a processor for infringing their rights as a result of the processor's non-compliance with the GDPR. Proceedings can be brought against a non-EU processor in the courts of the Member State where the individual resides. Additionally, there is no requirement for an individual to only proceed against the processor if the controller itself has factually disappeared, ceased to exist in law or become insolvent (as is the case under the 2010 controller to processor model clauses).

But a processor is only liable for damage to an individual if it has not complied with the processor-specific GDPR obligations or has contravened the controller's lawful instructions. Additionally a processor is exempt from liability if it can demonstrate that it is not responsible for the damage. But where a controller and processor are involved in the same processing, they are both held liable for the entire damage. As part of judicial proceedings, compensation may be apportioned according to who was responsible for the damage.

What Do These Changes Mean? A Few Probable Implications

1. **Changed relationships**. Being directly subject to the law affects the relationships that a processor has with individuals, controllers and with DPAs. Processors should consider how to manage this cultural change internally and externally as they interact with controllers. For example, since a processor is legally required to cooperate with the DPA, the processor will need to address how it complies with this obligation in a way that does not amount to a breach of contract with its controllers.

2. **Negotiations between controllers and processors**. In their negotiations with controllers, processors will not be able to object to responsibilities that they are directly required to comply with under the GDPR. This will affect both the ability of processors to negotiate certain points with controllers and the ability for processors to recover costs for time and resources spent helping controllers.

But processors will also want to ensure that they can comply with their own obligations under the GDPR. This means both that the controller should provide assistance to the processor with certain compliance requirements (such as compiling the records of processing) and that the controller should not instruct the processor to process personal data so that the processor breaches its obligations. The processor should also carefully consider the scope of the controller's instructions set out in the contract (and delivered as a result) since the processor can be liable for damage caused where it acts outside those instructions.

3. **Existing controller-processor agreements**. Once the GDPR comes into effect controller-processor agreements must include the specific provisions set out. A number but not all of these provisions may already be included in controller-processor agreements. But companies (both controllers and processors) will need to review their existing agreements and their standard terms to ensure that the documents comply. Where there is a gap, amendment agreements will be required.

4. **Engaging subprocessors**. Processors will have to find a viable way of seeking approval from controllers for all subprocessors appointed and flowing down the same contractual provisions to subprocessors. Managing this obligation in practice will depend on how complex the network of subprocessors is for processors. Certainly the right under the GDPR for a controller to object to a subprocessor is not bound by the requirement on the controller to act reasonably which could cause operational burdens for processors.

5. **Develop processor data privacy documents**. Processors will need to ensure that their internal documents meet the requirements of the GDPR and additionally give the controllers that engage them sufficient comfort. Adopting a Client Data Handling Policy which can be shared with customers and which sets out how the processor meets its obligations would be a prudent move.

6. **Handling data security breaches**. Processors are required to assist controllers with all the obligations surrounding data security breaches as well as notifying the controller if they become aware of a breach. Processors will probably be in a better position to describe the nature of the breach and the likely consequences and so help the controller provide the necessary information to the DPA. Additionally it will be processors who are likely to be better judges of whether the data that is the subject of a breach has been rendered unintelligible to third parties and thus avoid the requirement to notify affected individuals. To meet these requirements, processors should adopt a Data Incident Handling Policy that enables them to react quickly and consistently in the event of a data security breach.

But where a processor fails to implement appropriate security or fails to notify the controller without undue delay, a processor will be exposed to fines from DPAs of up to 10 million Euros ($11.1 million) or 2 percent of total worldwide annual turnover. Furthermore, a processor could face the prospect of class actions by individuals who seek compensation for damage that a processor has caused. These changes will require processors to carefully consider their liability and insurance arrangements to take account of this new environment.

Conclusion

EU law continues to distinguish between the roles of controllers and processors. But with the advent of the GDPR, processors will be subject to important further requirements which will require fresh ways of thinking

   ISSN 1473-3579

about compliance. All processors—from the big to the small—will need to come to grips with the new world of the GDPR.