Top 10 operational impacts of the GDPR: Part 7 - Vendor Management

Anna Myers, CIPM, CIPP/US

iapp

The General Data Protection Regulation (GDPR) is set to replace the Data Protection Directive 95/46/ec effective May 25, 2018. The GDPR is directly applicable in each member state and will lead to a greater degree of data protection harmonization across EU nations.

Although many companies have already adopted privacy processes and procedures consistent with the Directive, the GDPR contains a number of new protections for EU data subjects and threatens significant fines and penalties for non-compliant data controllers and processors once it comes into force in the spring of 2018.

With new obligations on such matters as data subject consent, data anonymization, breach notification, trans-border data transfers, and appointment of data protection officers, to name a few, the GDPR requires companies handling EU citizens' data to undertake major operational reform.

This is the seventh in a series of articles addressing the top 10 operational impacts of the GDPR.

Clarifying duties and responsibilities of controllers and processors

In its effort to protect and expand the rights of data subjects, the GDPR creates clear lines of accountability over data processing. This is especially evident in the way it delineates responsibilities between "controllers" and "processors" for handling personal data.

Under the Directive, data processors had duties of confidentiality and security. The Directive allowed them to act only with instructions from the controller, under contract, and to provide controllers with assurances of adequate technical and administrative measures to protect personal data.

The GDPR expands significantly upon the controller's responsibility for processing activities and sets out specific rules for allocating responsibility between the controller and processor.

The Regulation's more detailed requirements for controller-processor contracts may compel some data controllers to reassess their vendor agreements to achieve compliance. Processors not only have additional duties under the GDPR, moreover, they also face enhanced liability for non-compliance or for acting outside the authority granted by a controller. Nonetheless, the burden for personal data protection under the GDPR still rests primarily with controllers.

Burden on Controllers

The GDPR defines a controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data." The controller, therefore, is the entity that makes decisions about processing activities, regardless of whether it actually carries out any processing operations.

Article 24 makes controllers responsible for ensuring that any processing activities are performed in compliance with the Regulation. Controllers must "implement appropriate technical and organisational measures" not only not only to ensure compliance, but also to be able to demonstrate the measures that they have in place.

Controllers also have specific responsibility for:

- Carrying out data protection impact assessments when the type of processing is "likely to result in a high risk to the rights and freedoms of natural persons" and implementing appropriate technical safeguards.

- Assuring the protection of data subject rights, such as erasure, reporting and notice requirements, and maintaining records of processing activities.

- Duties to the supervisory authority, such as data breach notification and consultation prior to processing.

While the Regulation imposes these heightened requirements on controllers, it is important to note that it also relaxes one of the requirements that existed under the Directive. Controllers will no longer be required to register their processing activities with a Data Protection Authority (DPA) in each member state. Instead, the GDPR imposes strict requirements on controllers to maintain their own detailed records of processing.

The GDPR allows controllers to demonstrate their compliance with the Regulation by adhering to codes of conduct and certifications that were approved by DPAs in the relevant member states. The Regulation also encourages controllers to implement the principles of data protection by design and by default, where feasible. In essence, this means that controllers should design products with privacy in mind, rather than tacking it on as an afterthought, and that privacy-protective settings should be the default in any product.

Selecting processors

Controllers are liable for the actions of the processors they select and responsible for compliance with the GDPR's personal data processing principles. Under the GDPR, the term "processor" means a "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." In other words, while the controller is the entity that makes decisions about processing activities, the processor is any entity contracted by the controller for carrying out the processing. If a processor acts as a controller or outside the scope of authority granted by a controller, however, then the Regulation treats the processor as a controller for the relevant processing and it becomes subject to the provisions regarding controllers.

When selecting a processor, controllers must only use processors that provide sufficient guarantees of their abilities to implement the technical and organizational measures necessary to meet the requirements of the GDPR. For example, if a controller uses binding corporate rules or standard contractual clauses as an appropriate safeguard for cross-border data transfers, controllers should bind processors they select to those rules or terms. Unlike the Directive, which was largely silent on the matter, meeting the "sufficient guarantees" obligation can be accomplished under the GDPR through the use of an approved code of conduct or certification mechanism.

The controller should also consider carrying out a data protection impact assessment prior to selecting a processor. The Recitals suggest that such an assessment is prudent in all cases, but is particularly vital when the parties are handling sensitive personal data. The controller ignores at its peril signs that using a particular processor may involve high risk to personal data. The best approach if the controller wishes to proceed with that processor is to consult the relevant data protection authority first.

Once a processor is selected, the relationship between controller and processor should be governed by a contract or other legal act under Union or Member State law. The contract should contain provisions regarding the tasks and responsibilities of the processor. These provisions include how and when data will be returned or deleted after processing, and the details of the processing, such as subject-matter, duration, nature, purpose, type of data and categories of data subjects. The controller and processor may also choose to use standard contractual clauses adopted by the Commission.

Processors' additional duties and restrictions on subcontracting

The GDPR prescribes specific obligations of processors in addition to contract terms between controllers and processors. Processors' duties are primarily to controllers, including requirements to: (a) process data only as instructed by controllers; (b) use appropriate technical and organisational measures to comply with the GDPR; (c) delete or return data to the controller once processing is complete; and (d) submit to specific conditions for engaging other processors.

The processors' restrictions on subcontracting bear special attention. Under the GDPR, processors are prohibited from enlisting another processor without prior specific or general written permission of the controller. In either case, controllers retain the right to object to the addition or replacement of processors. Thus, if a processor enlists a subprocessor based on the controller's general consent, Article 28 requires the processor to inform the controller so that it may have the opportunity to object. Sub-processors also are subject to the same requirements under the GDPR and they too are bound by any contracts with the controller.

While the controller is responsible for maintaining records of processing activities, processors are responsible for maintaining records of all categories of personal data processing carried out on behalf of the controller. These records should contain contact information for the processor(s) and the controller(s), the categories of processing carried out for each controller, information on cross-border transfers if applicable, and a general description of the implemented technical and organizational security measures.

Joint controllers

Article 26 provides specific provisions for when "two or more controllers jointly determine the purposes and means of processing." Joint controllers are required to create an agreement determining their respective duties to comply with the Regulation. The agreement must be available to data subjects and may designate one point of contact amongst them for data subjects. Regardless of the allocation of responsibility set out in the contract, data subjects are entitled to enforce their rights against either controller. Therefore, each joint controller is individually liable for compliance with the Regulation.

Data breach responsibilities

In the event of a personal data breach, processors are required to notify the controller without "undue delay" if it happens on the processor's watch. The burden falls on the controller, then, to notify the supervisory authority within 72 hours of becoming aware of the breach. If notification is not made within 72 hours, controllers are required to provide a reasoned justification for the delay. Controllers are also responsible for documenting personal data breaches, including the facts of the breach, its effects, and remedial actions.

For more on this subject, see part 1 in this series.

Liability and penalties

Controllers are liable for the damage caused by processing "which infringes" the GDPR. Processors, on the other hand, are liable "only where it has not complied with the obligations of [the GDPR] specifically directed to processors or acted outside or contrary to lawful instructions of the controller." In other words, parties bringing claims against processors under the GDPR must prove an additional element apart from damage and general noncompliance, namely, that the processors have violated one of their specific legal duties or contractual obligations.

When non-compliance is established, the burden shifts to controllers and processors to prove they are not responsible for the damage in any way.

When the controller and processor are joined in the same judicial proceedings, liability for damages may be apportioned among them according to their respective responsibility for the harm, as long as the data subject(s) receive full compensation. Additionally, controllers or processors who have paid the entire compensation may institute proceedings against other controllers or processors involved in the same processing to claim back the portion(s) for which they are not responsible.

Where to find the rules

Looking to dive deeper into the General Data Protection Regulation to read the text regarding vendor management for yourself? Find the full text of the Regulation here in our Resource Center.

You'll want to focus on these portions:

Recitals

(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. 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.

(79) The protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and

measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes, and means of the processing jointly with other controllers or where a processing operation is carried out on behalf of a controller.

(81) To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject-matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

(84) In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to

result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours,the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(89) Directive 95/46/EC provided for a general obligation to notify the processing of personal data to the supervisory authorities. While that obligation produces administrative and financial burdens, it did not in all cases contribute to improving the protection of personal data. Such indiscriminate general notification obligations should therefore be abolished, and replaced by effective procedures and mechanisms which focus instead on those types of processing operations which are likely to result in a high risk to the rights and freedoms of natural persons by virtue of their nature, scope, context and purposes. Such types of processing operations may be those which in particular, involve using new technologies, or are of a new kind and where no data protection impact assessment has been carried out before by the controller, or where they become necessary in the light of the time that has elapsed since the initial processing.

(90) In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

(91) This should in particular apply to large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights. A data protection impact assessment should also be made where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special categories of personal data, biometric data, or data on criminal convictions and offences or related security measures. A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, especially when using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale. The processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer. In such cases, a data protection impact assessment should not be mandatory.

(92) There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or

processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

(93) In the context of the adoption of the Member State law on which the performance of the tasks of the public authority or public body is based and which regulates the specific processing operation or set of operations in question, Member States may deem it necessary to carry out such assessment prior to the processing activities.

(94) Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted, prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

(95) The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

(98) Associations or other bodies representing categories of controllers or processors should be encouraged to draw up codes of conduct, within the limits of this Regulation, so as to facilitate the effective application of this Regulation, taking account of the specific characteristics of the processing carried out in certain sectors and the specific needs of micro, small and medium enterprises. In particular, such codes of conduct could calibrate the obligations of controllers and processors, taking into account the risk likely to result from the processing for the rights and freedoms of natural persons.

(145) For proceedings against a controller or processor, the plaintiff should have the choice to bring the action before the courts of the Member States where the controller or processor has an establishment or where the data subject resides, unless the controller is a public authority of a Member State acting in the exercise of its public powers.

(146) The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other

rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation, may subsequently institute recourse proceedings against other controllers or processors involved in the same processing.

Articles

Article 4, Definitions

-2 processing

-3 restriction of processing

-7 controller

-8 processor

-9 recipient

-10 third party

Article 5, Principals related to processing of personal data

Article 6, Lawfulness of processing

Article 12, Transparent information, communication and modalities for the exercise of the rights of the data subject

Article 13, Information to be provided where personal data are collected from the data subject

Article 14, Information to be provided where personal data have not been obtained from the data subject

Article 17, Right to erasure ('right to be forgotten')

Article 24, Responsibility of the controller

Article 25, Data Protection by design and by default

Article 26, Joint controllers

Article 28, Processor

Article 29, Processing under the authority of the controller or processor

Article 30, Records of processing activities

Article 33, Notification of a personal data breach to the supervisory authority

Article 35, Data protection impact assessment

Article 36, Prior consultation

Article 82, Right to compensation and liability