GDPR – A guide to key articles for security & privacy professionals

SPONSORED BY

FORCEPOINT
POWERED BY Raytheon

HUNTON& WILLIAMS

TABLE OF CONTENTS

1. COVERAGE

This white paper outlines they key requirements of the General Data Protection Regulation. ("Regulation"). While many of the changes in the Regulation will affect data controllers and data processors, this white paper focuses on four obligations which will be critical for business. They are:

- The extended obligations related to the security of processing;
- The data breach notification duties;
- The right of individuals to the erasure of their personal data; and
- The rules covering transfers of personal data to third countries or international organisations.

2. UNDERSTANDING THE BACKGROUND

After a long process to update the European Union's data protection laws, the Regulation will enter into force on 25 May 2018. Final agreement on the Regulation was reached in April 2016 after a lengthy legislative process which took over three years to complete. The Regulation builds on the foundations of its predecessor, Directive 95/46/EC (the "Directive"), which has provided the basis for EU Member States' present data protection laws. While many of the provisions will look familiar, taken together, they will radically change the impact of data protection within the EU.

3. SCOPE OF THE REGULATION (ARTICLE 3)

The Regulation greatly expands the scope of EU data protection law, covering both controllers and processors that are established in the EU[1]. The specific coverage of data processors is a new development. In addition, the Regulation has extra-territorial effect and will apply to controllers and processors who are not established in the EU but supply goods or services to data subjects within the EU or carry out the monitoring of their behaviour[2].

4. SUPERVISORY AUTHORITIES AND THE EUROPEAN DATA PROTECTION BOARD

Every Member State must appoint an independent Supervisory Authority (SA). All SAs will have the same powers, including wide powers of investigation and the power to make mandatory orders against data controllers or processors in breach of the law. SAs will also deal with complaints by individuals. In addition, there will be a new pan-EU board composed of SAs, the European Data Protection Board (EDPB).

[1] Article 3.1
[2] Article 3.2

5. DEFINITIONS

The main definitions found in the Regulation reflect those in the Directive, including those of data controller and data processor. The definitions of data controller and data processor remain unchanged. There are, however, some changes to other existing definitions. For example, personal data is slightly more widely drawn and sensitive personal data has become "special category data", and includes some additional data categories. There are also some new definitions, such as profiling.

6. DATA PROTECTION PRINCIPLES (ARTICLE 5)

6.1 As with the Directive and the implementing Member State legislation, the core of the law is a set of strong principles. These are generally similar to the ones found in the Directive. The principles, which a data controller must be able to demonstrate compliance with[3], are the following:

- lawfulness (including the need for a legal ground to process personal data), fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage/retention limitation; and
- integrity and confidentiality.

6.2 Under Principle 1, the data controller must be able to show the legal grounds for processing personal data and additional grounds for processing special categories of personal data. These are largely the same as under the Directive. However, there is a major change to the standard of consent. Under the Regulation, "consent" means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to him or her being processed. Consent must be "unambiguous". The use of "unambiguous" means that implied consent will remain valid; however, it must be given by a "clear affirmative action" which indicates that some action on the part of the user is required (e.g., ticking a box when visiting an internet website or actively choosing technical settings).

Where consent is given in a document that also concerns other matters, the Regulation requires that the consent to processing personal data must be presented in a manner that is clearly distinguishable from the other matters. In other words, it cannot be hidden in the "small print"[4]. Where processing has multiple purposes, consent should be granted for all of the purposes. Where there is a significant imbalance between the parties, it is unlikely that consent can be freely given[5]. In such cases, there will be a presumption that consent is not valid.

[3] Article 5.2

[4] Article 7.2

[5] Recital 43

7. TRANSPARENCY AND NOTICE (ARTICLE 12)

The Regulation requires more detailed notice than does the Directive. In addition to information about the data controller, the data itself and the purposes of the processing, the following information must be provided to data subjects:

- the details of any data protection officer ("DPO");
- the legal basis relied upon;
- the recipients or categories of recipients; and, where relevant,
- information on cross-border transfers of the data.

  In addition, further information must be given where it is relevant, being:
  - where data are processed on the basis of legitimate interests, the legitimate interests pursued by the controller or third party;
  - where data are processed on the basis of consent, the existence of the right to withdraw consent at any time;
  - the applicable data retention period;
  - the existence of the rights of data subjects, the right to complain to the Supervisory Authority ("SA");
  - whether the provision of personal data is a statutory or contractual requirement, or a requirement to enter into a contract, and whether the data subject is obliged to provide the data and the possible consequences of a failure to provide such data; and
  - the existence of automated decision taking including profiling and meaningful information about the logic involved, and the envisaged consequences of such processing for the data subject.

8. SECURITY OF PROCESSING (ARTICLE 32)

8.1 Personal data must be processed in a manner that ensures appropriate security of the personal data. This will include protection against unauthorised or unlawful processing, as well as against accidental loss, destruction or damage, using appropriate technical or organisational manners. The obligation is placed on both the controller and the processor, and both will need to keep records of the measures in place. Article 32 provides a non-exhaustive list of security measures, both technical and organisational, that could be used to safeguard personal data as appropriate. These are:

- the pseudonymisation and encryption of data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

8.2 Assessment of the appropriate level of security to implement must take into account the risks attached to the processing. Recital 39 states that personal data should be processed in a way that ensures appropriate security and confidentiality of the data. This includes preventing unauthorised access to or use of personal data and the equipment used for that processing. Controllers must ensure that the processors they use are able to provide satisfactory security guarantees. Where a processor cannot show that it has in place appropriate technical and organisational safeguards, then the controller should not engage them.

8.3 **Risk assessment**

As explained, the Regulation will apply to both data controllers and data processors, making data processors across the EU directly liable for their personal data processing activities[6]. The imposition of direct legal obligations, as well as those imposed by contract with the data controller, will mean increased risks, as such obligations can be directly enforced by SAs and also give rise to actions by data subjects. Controllers and processors should therefore evaluate the risks inherent in their processing and implement measures to mitigate those risks, such as encryption. They must consider the state of the art and the associated implementation costs in respect to risk mitigation and the nature of the personal data to be protected. The nature of the processing itself, such as whether data are transmitted, stored or otherwise processed, will also impact the risk posed by the processing and determine the appropriate level of security.

8.4 **Action points**

- *Undertake review of organisation's risk dynamic for all forms of processing*
- *Establish/update detailed information security policies and procedures covering both organisational and technical measures*
- *Consider seeking certification to demonstrate security credentials*

[6] Articles 3 and 28

9. THIRD PARTY CONTRACTING (ARTICLE 28)

9.1 Data controllers may engage only processors that provide adequate security guarantees. Contracts must set out the subject matter, duration of processing, and the obligations and rights of the controller. In addition, the processor must agree to some specific contractual obligations, requiring them to[7]:

- process personal data only on the instructions of the controller, including the transfer of data to third countries;
- ensure that staff are bound by confidentiality;
- ensure the security of the data;
- only use sub-processors with the consent of the controller;
- assist with the handling of individual rights;
- assist with complying with security and breach requirements;
- return or delete all personal data at the end of the contract; and
- allow audits and other monitoring to prove compliance.

Any sub-processing must be subject to the same obligations that are included in the head contract and it is the processor's responsibility to ensure that such a contract is entered into[8].

[7] Article 28.2
[8] Article 28.4

10. ACCOUNTABILITY (SECURITY BREACH NOTIFICATION) (ARTICLES 33 AND 34)

10.1 Security breach notification must be appreciated in the wider context of the new "accountability" obligations under the Regulation. These obligations mean that controllers must be able to show that they are meeting the required standards.

10.2 The Regulation requires controllers to implement appropriate measures to be able to demonstrate compliance with the provisions of the Regulation. Article 5.2 imposes a general obligation that controllers must be able to demonstrate compliance with the principles. In addition, there are a number of specific requirements to demonstrate accountability:

- Internal records of processing activities[9]: These have to cover details of the controller and any joint controller; the DPO, if any, the purpose of the processing; data subjects and data categories; recipients and transfers; retention periods and security policies.

- Data Protection Impact Assessment[10]: If a proposed new data processing activity is likely to result in a high risk for the data subjects' rights or freedoms, controllers must conduct a data protection impact assessment (DPIA), in order to thoroughly consider those risks and identify possible solutions. The DPIA must contain, amongst other things: a description of the processing and its purposes; an assessment of the necessity and proportionality of the processing; and an evaluation of the risks related to the processing and the measures envisaged to address these risks. The Regulation contains a list of specific processing activities which will require a DPIA, such as the processing of sensitive personal data on a large scale. SAs may further expand this list.

- Prior consultation[11]: In cases where the DPIA shows that the processing would result in a high risk for the data subjects and no measures will be taken to address those risks, controllers must consult the SA before initiating the concerned processing activity.

- DPO[12]: There is an obligation to appoint a DPO if the organisation is a public authority or if the core activities of the controller involve large scale regular and systematic monitoring of individuals or processing personal data in the special categories, or about criminal convictions or offences. The role of the DPO is significant. If one is required, it is important to have the necessary documents and structures in place to enable the organisation to demonstrate that the DPO can fulfil its role.

- Data Protection by Design and Default[13]: The principles of Privacy by Design and Privacy by Default, which currently exist as "best practices", will become explicit legal obligations under the Regulation. These principles require data controllers to properly assess and take into account data protection issues from the start of the design process of any product, service or technology. Data controllers must, both at the point of developing or designing a new processing operation (e.g. a new technology, product or service), and when carrying out the processing, do so in a manner which ensures compliance with data protection obligations and

[9] Article 30
[10] Article 35
[11] Article 36
[12] Article 37
[13] Article 20

adequately protects data subjects' rights. This may require adopting additional measures such as encryption.

- Codes of Conduct[14]: The Regulation introduces approved codes of conduct and certification mechanisms as an authorised way of demonstrating an organisation adheres to high standards of data protection. Organisations should therefore consider applying for certification or signing up to approved codes of conduct once these have been developed.

10.3 **Security Breach Notification**

Security breach notification is one of the most important aspects of the new accountability regime (Articles 33 & 34). It is in this wider context that the new mandatory breach notification has been imposed. In some cases, data security breaches that affect personal data will require notification of the competent SA and also the affected data subjects.

10.4 **Notifiable breaches**

A breach will be notifiable if it is a "personal data breach". This is defined as:

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed[15].

This is a broad definition and it reinforces the importance of having appropriate security safeguards in place and the correct accountability systems to recognise when such a breach has taken place and to report it appropriately.

10.5 **Notification to the Supervisory Authority**

If a data controller suffers a personal data breach, the controller must notify the competent SA without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach[16]. This will be the SA for the place where the breach occurs. If the SA cannot be notified within 72 hours, the controller must provide an explanation of the reasons for the delay together with the notification to the SA. If it is impossible to provide all the required information on the personal data breach immediately, the controller may provide the information in different phases. The notification must contain at least the following information[17]:

- the nature of the breach, including the categories and approximate number of affected data subjects and data records;
- the name and contact details of the DPO or another contact point where information concerning the breach can be obtained;
- the likely consequences of the breach; and
- the measures taken or proposed to be taken to address the breach and mitigate its possible adverse effects.

Notification to the SA is not required only if the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals (e.g., if the data were encrypted). It will be critical that data controllers are able to ascertain with certainty whether personal data were encrypted or otherwise protected.

10.6 **Record keeping**

Controllers must also keep internal records of any personal data breaches, containing a description of the facts surrounding the breach, its effects and the remedial actions that were taken[18].

[14] Article 40
[15] Article 4
[16] Article 33.1
[17] Article 33.3
[18] Article 33.5

10.7 **Notification to affected data subjects**

In those cases where the personal data breach is likely to result in a high risk for the rights and freedoms of these individuals, controllers must notify affected individuals without undue delay[19]. Notification should be made as soon as reasonably feasible. The notification to the data subjects will need to include the name and contact details of the DPO or another contact point where data subjects can obtain more information on the breach. Furthermore, the notification will need to provide a description of the likely consequences of the breach and the measures taken or proposed to be taken to address the breach, in clear and plain language. Notification is not required if the controller[20]:

- has implemented appropriate technical and organisational security measures to protect the affected personal data, in particular, measures which render the affected data unintelligible for unauthorised individuals;
- has taken subsequent measures which ensure that the high risk for the data subjects' rights and freedoms is no longer likely to materialise; or
- it would involve a disproportionate effort - in which case releasing a public communication or taking a similar measure to effectively inform the data subjects will be required.

Even in cases where the controller considers that no notification to the data subjects is required, the SA may still order such notification.

10.8 **Data processors**

Processors must notify the controller of security breaches that affect personal data and those individuals on whose behalf they are processing the affected data, without undue delay[21]. No hard timescale is fixed, but since data controllers must notify the SA with 72 hours, the notice should be given in sufficient time to allow data controllers to make their notification.

10.9 **Action points**

- *Create a system for logging detailed records of data breaches*
- *Draft and implement breach response policies and procedures*
- *Create a breach response team with relevant stakeholders represented*
- *Develop templates for notifications to SAs and data subjects*
- *Run mock data breaches/table top exercises to prepare for breaches and test procedures*
- *Consider/review insurance coverage for data breaches*
- *Review third party contracts with service providers to ensure liability provisions cover data breaches*
- *Introduce technical controls to detect and monitor the system for destruction or loss of, and unauthorised access to, personal data and to flag such events*

[19] Article 34.1
[20] Article 34.3
[21] Article 33.2

11. RIGHT TO ERASURE AND OTHER DATA SUBJECT RIGHTS (ARTICLES 15-21)

11.1 The right to erasure of personal data is one of a number of rights in the Regulation and may have a very significant effect on data controllers. Individuals will have the right to complain about any breach to an SA, usually this will be the local SA. If an SA does not act on their complaint and deal with it properly, they can take action against that SA. Data subjects may also seek orders to enforce their rights from the courts and compensation before the courts for any breach that has caused them "damage". Individuals can be represented by representative organisations, which is likely to allow them to bring "legal class actions" where there has been a breach[22].

11.2 Articles 15-21 provide for strengthened and new rights for data subjects as described below:

- Subject access[23]: Data subjects have the right to subject access in relation to data processed by controllers within 1 month of making a request. The subject access right is broadly similar to the current right under the Directive. Data subjects have the right to obtain confirmation as to whether data relating to them are being processed, and to receive the following information:
  - the purposes of the processing;
  - the categories of personal data processed;
  - the recipients to whom personal data have been disclosed;
  - the period for which personal data will be stored;
  - the existence of a right to request rectification or erasure of personal data from the controller;
  - the right to lodge a complaint with the SA, and receive the contact information of the SA;
  - where the data are not collected from the data subject, information as to their source;
  - the existence of automated decision making, including profiling, meaningful information as to the logic involved, and the significance and consequences of that processing for the data subject; and
  - where the data have been transferred to a third country, the appropriate safeguards that have been implemented in respect of the transfer.

They must also be provided with a copy of personal data relating to them that are being processed by the controller.

- The Right to Restrict Processing ("RtRP")[24]: The Right to Restrict Processing of personal data is a new right that will allow data subjects to request data controllers to limit the purposes for which relevant personal data are processed but not to have it erased. It applies where:
  - the accuracy of the data is contested by the data subject; in such a case, the restriction only applies for as long as it takes the controller to verify the accuracy of the data;
  - the processing is unlawful and the data subject requests restriction of the use of the data, rather than their erasure;
  - the controller is holding the data in case of future legal action; or
  - the data subject has objected to the processing and the controller is in the process of verifying whether that objection is valid. This provision will enable data subjects to seek an immediate restriction of processing pending a determination on the merits of a request for erasure.

[22] Article 80
[23] Article 15
[24] Article 18

- The Right to Object ("RtO")[25]: Data subjects can object to any processing of personal data. In certain cases, data controllers must accept such objections and act on them. Data subjects continue to have an absolute right to object where the processing is carried out for the purpose of direct marketing. They will also have a more general right to object where the legal basis of the processing is either: the performance of a task carried out in the public interest or the exercise of official authority under a discretionary power, or the processing is being carried out for the legitimate interests of the controller, which are not out-weighed by any detriment to the rights and freedoms of the data subject.

- The Right to Rectification: The Right to Rectification applies where personal data are inaccurate. Data subjects also have the right to obtain "completion" of the data where the data are incomplete. This may be achieved, for example, by adding a supplementary statement.

11.3 **The Right to Erasure of Personal Data**[26]

As has been explained, this is one of a number of rights for individuals, but this right to require the controller to delete their personal data will raise new challenges for data controllers.

The right to erasure applies where[27]:

- the data are no longer necessary in relation to the purposes for which they were collected;
- the processing is based on the data subject's consent and the data subject withdraws that consent;
- the data subject has successfully exercised the right to object to the processing (see the explanation above);
- the data have been unlawfully processed;
- the controller is under a legal obligation to erase the data; or
- the data have been collected in relation to the offering of information of society services to a child.

There are a number of exceptions when the data controller does not have to accept the request to erase personal data (freedom of expression and of information; compliance with a legal obligation; public interest in the area of public health; some archiving purposes and the establishment, exercise or defence of legal claims[28]). Some of these exemptions are to be established by Member State law, therefore the scope and the detail will vary from jurisdiction to jurisdiction.

Where a request for erasure has been accepted, erasure must be carried out without undue delay. Moreover, if the controller has made the data public, it must take reasonable steps to inform other controllers processing the data that the subject has requested the erasure of links, copies or replicas of the data[29].

Where necessary, the data subject's exercise of their right to erasure must be communicated to third party recipients to whom the organisation has disclosed the personal data. If a controller denies the request for erasure, the data subject may request that the national SA verify the lawfulness of the processing.

Where the individual is not entitled to erasure, as in cases where the data subject contests the accuracy of personal data and its accuracy or inaccuracy cannot be ascertained, or the data must be maintained for evidential purposes, the data subject will be entitled to restrict processing. Processing can also be restricted in cases where the data subject does not wish to have the data erased because it is required for the purposes of establishing the legal rights of the data subject[30].

[25] Article 21
[26] Article 17
[27] Article 17.1
[28] Article 17.3
[29] Article 17.2
[30] Article 18.1

The right to erasure would seem to extend to back-ups of data; however there is a central conflict between the data subject's right to erasure and any requirements to maintain records for evidential purposes. In such circumstances, a practical solution may be to take measures to restrict processing or block access to the personal data in question.

11.4 **Action points**

- *Review systems and make any adjustments necessary to ensure that personal data can be easily deleted from the systems on request;*
- *Where sharing personal data with processors or other third parties, put in place practices and procedures to allow the tracking of personal data in order to comply with any requests for erasure at a later date;*
- *Ensure that arrangements, contractual and organisational, are in place so that third parties holding any personal data of which the data subject has made an erasure request can be deleted without undue delay.*

12. DATA PORTABILITY (ARTICLE 20)

The new right to data portability enables data subjects to obtain their personal data in a structured, commonly-used and machine-readable format from a data controller and transmit it to another (for example, a data subject could ask to transfer their personal data from Facebook to another social media platform). The right applies where (i) the processing is based on consent or is necessary for entering into or performance of a contract, and (ii) the processing is carried out by automatic means. Data subjects may also require one controller to transfer data directly to the other controller, "where technically feasible".

13. PROFILING (ARTICLE 22)

13.1 The Directive applies to automated decision making about individuals in some circumstances, but does not deal specifically with profiling. Under the Regulation, profiling is defined as any automated processing of personal data consisting of using those data to evaluate certain personal aspects related to a natural person, in particular, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements[31].

13.2 Profiling can be a component part of the activity of monitoring individuals. The definition potentially covers an extremely wide range of activities. Any analysis or prediction (e.g., this person is likely to be interested in holidays in Ireland) is caught by the definition.

Profiling is not banned but it is treated as an activity which carries risk and which may be intrusive into the privacy of the data subject. Therefore, there are restrictions on how profiling can be used, and individuals have clear rights to object to profiling activities. As a distinct form of processing, the controller must be able to show clear grounds (e.g. legitimate interest) on which it is entitled to carry out profiling. The EDPB can issue further guidelines on how the Regulation applies to processing. It is likely, therefore, that detailed guidance will be issued in the future.

[31] Article 4

14. DATA TRANSFERS (ARTICLE 44-50)

14.1 As is the case under the current regime, there is a general prohibition on transfers of personal data to jurisdictions outside the European Economic Area (EEA) unless the conditions for transfer are met (e.g., Model Clauses, adequacy determinations and BCRs). The Regulation goes further, however, stipulating that onward transfers must be covered by adequate protection in addition to the initial transfer outside the EEA[32].

14.2 There are limited legal derogations for transfers of personal data to jurisdictions outside the EEA. These are similar to those in the Directive and apply where no other mechanism to guarantee adequacy is applicable[33]. The derogations are:

- explicit consent of the data subject. For the consent to be valid, the data subject must have been informed of the risks of the transfer;
- the transfer is necessary for the conclusion or performance of a contract with the data subject or in the data subject's interest;
- the transfer is necessary to protect the vital interests of a data subject;
- the transfer is necessary in the public interest or to exercise or defend legal claims;
- the transfer is made from a public register;
- the transfer is in the controller's legitimate interests. This ground can be used only in the most limited circumstances, those being that a) the adequacy tests cannot be satisfied b) none of the safeguarding mechanisms can be used and c) no other derogations are applicable. The transfer cannot be repetitive, must concern only a limited number of data subjects, and must be necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests of the subject. In addition, safeguards must be in place; the SA must be informed and notice of the transfer and the interests must be given to the data subjects.

In additions to legitimate interests, derogation provides a potential "last resort" for data exporters; it is important, however, that organisations view it as such. The derogation is very restrictive and the notification requirements for those invoking the derogation reduce its practicability. In addition, if a controller relies on legitimate interests to transfer personal data to a non-adequate country outside the EEA, the assessment made regarding the circumstances surrounding the transfer and the data protection safeguards in place must be documented and retained.

14.3 **Binding Corporate Rules**

Binding Corporate Rules ("BCRs") are formally recognised in the Regulation, which also provides a single approval mechanism for BCRs under the Consistency Mechanism[34]. It should be noted that:

- BCRs can apply to groups of undertakings engaged in joint economic activity;
- BCRs are available for processors (Art 4.17 definition of BCRs); and
- BCRs are only available to data exporters (whether controllers or processors) that are established in the EU.

[32] Article 44
[33] Article 49
[34] Article 47.1

Article 47 of the Regulation outlines the requirements BCRs must satisfy before SAs can approve them under the Consistency Mechanism. BCRs must:

- be legally binding and apply to and be enforced by all members of the group of undertakings or group of enterprises engaged in joint economic activity (together, "Groups"), including their employees;
- expressly confer enforceable rights on data subjects with regard to the processing of their personal data;
- specify the structure and contact details of Groups and each of their members;
- specify the data transfers, or set of transfers, including details of the processing involved (i.e. categories of personal data, type and purpose of processing, data subjects affected) and the third countries in question;
- clarify the BCRs' legally binding nature, both internally and externally;
- specify the application of the general data protection principles;
- outline the rights of the data subjects in respect of the processing;
- State whether the controller or processor established within the territory of an EU member state accepts liability for breaches of the BCRs by any member concerned not established within the EU;
- explain how the information on the BCRs is provided to data subjects in addition to notice requirements;
- outline the tasks of any DPO or any other person or entity responsible for monitoring compliance with the BCRs;
- specify the complaint procedures in place;
- explain the mechanisms in place within the Group to verify compliance with the BCRs;
- detail the mechanisms for reporting and recording changes to the BCRs and procedures for notifying the SA of these changes;
- specify the cooperation and reporting mechanisms with respect to the SA; and
- explain the data protection training personnel will receive if they have regular access to personal data in their roles.

Anyone familiar with the existing BCR regime will appreciate that the process of having BCRs approved by SAs is rigorous and time-consuming. The codification of the requirements, however, may improve the efficiency with which BCR approvals are made by further harmonising the process.

14.4 **Adequacy determinations**

The Commission may make findings that the legal regime in another jurisdiction provides equivalent protection to that in the EU. Such adequacy findings can be made in relation to a third country or territory, as well as for specific sectors in a third country or international organisations. The findings are implemented by secondary EU legislation, which must provide a mechanism for periodic review and specify the territorial or sectoral application[35]. Transfers made on the basis of an adequacy determination do not require further approval or authorisation from an SA.

The Commission has an ongoing obligation to monitor the situation in any area where it has made an adequacy finding[36].

Because adequacy is monitored on an ongoing basis, controllers and processors are recommended to stay up to date with the status of each country to which they export data. If a country or territory loses its adequacy status, then transfers will be invalid unless a safeguard is put in place to validate the transfer.

[35] Article 45
[36] Article 45.4

14.5 **Model Clauses, Codes of Practice and Certification**

Model clauses (controller to processor and controller to controller) can be adopted by the Commission or adopted by SAs and approved by the Commission[37]. Model clauses remain widely used by organisations transferring personal data outside the EEA. The existing clauses prepared by the Commission will remain available when the Regulation comes into force[38]. There remains a gap for processor to processor transfers, which may be more widely felt once the Regulation comes into force, with the transfer restrictions imposed on processors. A set of processor to processor model clauses are expected to be produced by the Commission.

The Regulation dispenses with the requirement of prior notice or prior approval from the SA where Model Clauses are used. A number of EU Member States implemented such requirements, which have added layers of bureaucracy and tended to make the use of Model Clauses a difficult exercise. This will be a welcome development for many organisations with pan-EU operations.

Ad hoc clauses must be approved by SAs[39]. This will allow SAs to ensure that all contractual arrangements meet the minimum standards set out in the Regulation.

The use of approved codes of practice and certification mechanisms will be additional mechanisms which can be used to establish the adequacy of transfers made under contractual arrangements[40].

14.6 **Third country requirements**

Any judgment of a court or tribunal or order of an administrative authority in a third country requiring the transfer or disclosure of personal data will only be enforceable if it is based on an international agreement, such as a Mutual Legal Assistance Treaty (MLAT)[41].

This is likely to continue to create conflicts for organisations that are issued with disclosure orders in third countries with which they must comply under local laws. Many disclosure laws impose substantial sanctions on organisations that fail to comply with such orders. Under the Directive, many organisations have opted to fully comply with disclosure orders while complying as far as reasonably possible with EU data protection laws, often basing decisions on economic rationale. The significant rise in monetary penalties available to SAs under the Regulation (see section 16), however, will reset the balance, making such decisions considerably harder for organisations.

14.7 **Action points**

- *Perform a complete analysis of all data flows from the EEA and establish in which non-EEA countries processing will be undertaken.*
- *Review cloud service agreements for location of data storage and any data transfer mechanism, as relevant.*
- *Ensure that an appropriate measure, such as Model Clauses or BCRs, is in place for any transfers to countries that are not deemed adequate by the European Commission.*

[37] Article 46.2(c) and (d)
[38] Article 46.5
[39] Article 46.3
[40] Article 46.2(e) and (f)
[41] Article 50

- *Ensure that appropriate onward transfer safeguards are in place where an organisation receiving the controller's personal data uses sub-contractors to carry on business.*
- *Monitor adequacy status of importing countries or territories.*

15. SUPERVISORY AUTHORITIES AND THE ONE STOP SHOP (ARTICLES 51-66)

15.1 Controllers and processors will be subject to the authority of the SA for any jurisdiction in which they have an establishment[42]. This means that controllers or processors which have establishments in more than one EU jurisdiction will be subject to more than one SA. In such cases, the Regulation provides for controllers or processors to work with a primary or lead SA in respect of cross-border processing[43]. Cross-border processing is defined as processing which takes place in establishments of the controller or processor in more than one Member State, or processing which takes place in the context of one establishment but which affects individuals in more than one Member State[44]. The appointment of a lead SA is intended to simplify administration and enforcement and to provide a mechanism for consistency in cases where the processing carried out by one controller affects individuals in more than one Member State.

15.2 The controller or processor will work with the SA for the main establishment where cross-border processing is involved ("lead SA"). If they have a single establishment but their processing affects other data subjects in the EU, the SA of the place of single establishment will be treated as the lead SA for cross-border processing. Local cases will continue to be handled by the SA for the specific jurisdiction[45].

15.3 Although there will be a lead SA in cross border cases, all the concerned SAs, that is, SAs in jurisdictions where a controller or processor has another establishment or data subjects are affected or potentially affected by the processing in question, will have a say in significant decisions on enforcement[46]. Consultation will take place between concerned SAs to achieve an agreed outcome in any enforcement matter. If the concerned SAs cannot agree on an appropriate decision, it is referred to the EDPB, which will make the final decision[47]. The decision of the EDPB is then remitted to the relevant lead SA to enforce against the data controller or processor.

15.4 Where a controller or processor is not established in the EU but is otherwise subject the Regulation, it will not be able to have a main establishment or a lead SA.

[42] Article 55.1
[43] Article 56.1
[44] Article 4
[45] Article 56.2
[46] Article 60-63
[47] Article 60.4, 63 and 65

16. FINES AND PENALTIES (ARTICLES 83-84)

Supervisory Authorities will have wide powers, which are very similar to those most EU SAs have under the current law[48]. They will also be able to make mandatory orders, which is similar to the powers of the Information Commissioner's Office (ICO) in the UK[49]. In addition, they will have very significant fining powers for a wide range of breaches of the Regulation. The fines can be issued against any data controller or processor, whether a corporate body, an association or an individual. There are two levels of fine: the lower level has a maximum of 10 million euros or, in the case of an undertaking, up to 2% of annual worldwide turnover, whichever is the higher[50]; the higher level has a maximum of 20 million euros or, in the case of an undertaking, of up to 4% of annual worldwide turnover, whichever is higher[51]. It should be noted that the percentage maximum levels apply only to "undertakings", that is, entities which engage in economic activity. An entity which is not an undertaking will be subject to the fixed maximum levels. There are also specific provisions for public bodies. It is for Member States to lay down the rules on whether and to what extent, administrative fines may be levied on public bodies established in the Member State.

17. CONCLUDING THOUGHTS

17.1 The Regulation entered into force in May of 2016. There is a two year time period before it applies[52]. A year has already passed, so businesses and other organisations now have twelve months before they must be able to comply in May of 2018. Over the next twelve months, data controllers and processors should be focusing on the issues which are critical for business in preparation for May 2018. They should also be aware of the wider context for data protection change. The Regulation is not the only part of the data protection and privacy regime under review. Although those areas covered by Directive 2002/58/EC in relation to processing of personal data in connection with the provision of publicly available telecommunications in the EU are not affected[53] by the Regulation, that Directive itself is under review and likely to be replaced.

17.2 In due course, the Commission may also bring out further proposals to keep the Regulation up to date in response to the changing technological environment[54]. This possibility follows on from the duty of the Commission to evaluate and review the way that the Regulation is working. It must submit its reviews and evaluations to the European Parliament and the Council every four years after the Regulation enters into force. The first review will therefore take place in 2020.

[48] Article 58.1
[49] Article 58.2
[50] Article 83.4
[51] Article 83.5
[52] Article 99
[53] Article 95
[54] Article 97.5

ABOUT THE AUTHOR

Rosemary Jay is a senior consultant attorney at Hunton & Williams. She joined from Pinsent Masons LLP, where she was head of the Information Law Practice. Prior to that she was the head of the Legal Office of the Data Protection Registrar (now the Information Commissioner) for 12 years. She has practiced in privacy law for nearly 30 years and is recognized as one of the top lawyers in the area of data protection in the UK, with Chambers and Partners consistently recognizing her as a top tier lawyer in data protection. She advises on high-level privacy, data protection and confidentiality issues. She has advised non-EU states on the adoption and drafting of privacy laws.

Rosemary is author of Data Protection Law & Practice (Sweet & Maxwell 4th edition 2012), and a Guide to the General Data Protection Regulation (Sweet & Maxwell February 2017) and a contributing editor to The White Book on data protection. She is a Fellow of the British Computer Society and was named Internet and E Commerce Lawyer of the Year 2017 by Finance Monthly. She has worked with the Council of Europe and the European Commission on privacy issues in Europe and the Commonwealth Secretariat in West Africa. Rosemary speaks on data protection frequently and is a regular contributor to journals, conferences and workshops, as well as participating on a number of advisory committees in the area of privacy and data protection. She has a particular interest in training and the development of effective training materials.

ABOUT THE SPONSOR

Forcepoint's portfolio of products safeguards users, data and networks against the most determined adversaries, from accidental or malicious insider threats to advanced outside attacks, across the entire threat lifecycle.

Specific to GDPR, Forcepoint provides organizations with deep visibility into how critical data is being processed across their infrastructure; on-premises, in the cloud or within their increasingly remote workforce.

Forcepoint's data protection and insider threat technologies not only provide the ability to monitor, manage and control data at rest, in use and in motion, but they also utilize user behavior analytics and machine learning to discover broken business processes and identify employees that elevate risk to critical data.

There are three core areas where Forcepoint's solutions can help organizations meet the requirements of GDPR:

- Support and maintain an accurate personal data inventory, whether as part of the initial scoping of a compliance program or to support the operational duties of controllers, processors or responders, including dealing with subject access requests or data incidents.

- Support the mapping of personal data flows across the organization that expose broken business processes and unsanctioned IT or highlight supply chain activity that puts critical data at risk. This clear visibility allows organizations to implement management and control of personal data flows using mechanisms such as authorization, policy-based encryption, notification and blocking to mitigate risk.

- Leveraging behavioral analytics and risk modelling to rapidly detect high risk employee activity (malicious or compromised) and broken business processes that put critical data at risk, as well as enabling a quick and decisive response, which often lets organizations get ahead of the breach itself.

FOR MORE INFORMATION ON GDPR, VISIT: WWW.FORCEPOINT.COM/GDPR

Protecting the human point.

SPONSORED BY

FORCEPOINT
POWERED BY Raytheon

HUNTON& WILLIAMS