crowell moring

The new European

GENERAL DATA PROTECTION REGULATION

GDPR

INTRODUCTION

The protection of individuals in relation to the processing of their personal data is a European fundamental right laid down in Article 8 (1) of the Charter of Fundamental Rights of the European Union and Article 16 (1) of the Treaty on the Functioning of the European Union. Businesses that want to process personal data of EU residents must therefore respect strict rules and conditions.

These rules and conditions are now predominantly laid down in the new EU General Data Protection Regulation (GDPR). The GDPR replaces the EU's 20-years-old Data Protection Directive (95/46/EC) and the 28 national laws of the EU Member States that implemented this Directive.

The aim of the GDPR is to provide a uniform law that strengthens the rights of individuals with regard to the processing of their personal data while at the same time facilitating the free flow of data in the digital single market and reducing the administrative burden for businesses.

The GDPR is not only important for all businesses that are established in Europe, it also affects businesses that do not have a European presence but offer goods or services to individuals in Europe or monitor the behavior of those individuals.

This guidance paper is not legal advice, but aims to provide businesses worldwide with a useful tool to further their understanding of the key aspects of the GDPR. It is not, and nor is it intended to be, exhaustive. Please see it as a first step in your path to compliance and feel free to contact us so that we can help you build up your overall compliance strategy taking into account your particular circumstances.

Crowell & Moring

www.crowell.com

INDEX

1. THE GDPR – A SHORT HISTORY

European data protection law was first harmonized in 1995 by the Data Protection Directive 95/46/EC (the 1995 Directive). An EU Directive, however, does not have direct effect in the Member States and instead has to be implemented into national laws. This has resulted in the current patchwork of 28 similar, but different, national laws in the various EU Member States.

More than 20 years later the new GDPR aims at harmonizing the data protection rules in the EU by creating *"a single set of rules, instead of 28"*, based on a Regulation that has direct effect in the Member States and does not require national implementation.

The GDPR was intended to modernize laws which had been written in the early days of the Internet. While it builds on the concepts, rights and obligations set out in the 1995 Directive, it also provides further details and adds new elements. Of particular significance is the inclusion of sanctions intended to support the enforcement of these rights and obligations.

The European Commission initiated the reform process in 2012 and it took almost 4 years for a political agreement to be reached on the new GDPR on December 15, 2015.

The GDPR was finally adopted on April 27, 2016 and was published in the Official Journal of the European Union on May 4, 2016. It entered into force 20 days later, and will apply as from May 25, 2018 after a two years' transition period.

WHAT DOES THIS MEAN FOR YOUR BUSINESS?

By 2018 all businesses will have to have fundamentally changed their data protection practices to ensure that their processes, policies and contracts all conform to the new Regulation.

2. SPECIFIC WORDING IN THE GDPR

Below we briefly explain some important wording used in the GDPR. These explanations are not exact copies of the definitions in the GDPR. For the legal definitions, we refer to **Article 4** of the GDPR.

Personal data	Any information relating to an identified or identifiable natural person.
Data subject	An identified or identifiable natural person (anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name or ID card).
Processing	Any operation performed on personal data, manually or automatically, from the collection of the data to its destruction.
Controller	An individual or an entity which alone, or jointly with others, determines the purposes for and means of processing the personal data.
Processor	An individual or an entity which processes personal data on behalf of a controller.
Recipient	A person, company, authority or body to which personal data are disclosed.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Pseudonymisation	The processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.
Special categories of personal data (= sensitive data)	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data, data concerning health or sex life or sexual orientation.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of an individual, allowing or confirming the unique identification of that individual (such as facial images).
Genetic data	Personal data relating to the inherited or acquired genetic characteristics of an individual, which give unique information about the physiology or health of that individual.
Data concerning health	Personal data related to the physical or mental health of an individual.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data.
Data protection officer (DPO)	An individual to be appointed by certain controllers or processors to *i.a.,* inform and advise the controller and processor and their employees on the GDPR and to monitor compliance.
European Data Protection Board (EDPB)	A body composed of the head of one supervisory authority of each Member State and the European Data Protection Supervisor. The EDPB replaces the current "Article 29 Working Party".
Supervisory authority (SA)	An independent public authority in a Member State responsible for monitoring the application of the GDPR. Equivalent to the current "data protection authority" (DPA).

3. MATERIAL AND TERRITORIAL SCOPE

3.1 Material Scope

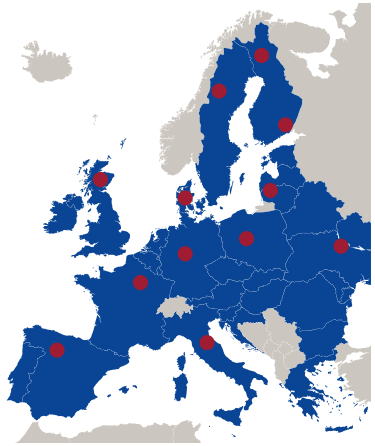
The GDPR generally applies to all processing of personal data:

- wholly or partly by automated means, and
- other than by automated means as part of a filing system or when intended to form part of a filing system.

3.2 Territorial Scope

PROCESSOR OR CONTROLLER WITH ESTABLISHMENT IN THE EU

The GDPR applies to the processing of personal data in the context of activities of an **establishment of a controller or a processor** in the EU, regardless of whether or not the processing itself takes place within the EU.



● = establishment of controller / processor

PROCESSING WITHOUT ESTABLISHMENT IN THE EU BUT REGARDING DATA SUBJECTS IN THE EU

The GDPR also applies to the processing of personal data of **data subjects who are in the EU,** by a controller or processor not established in the EU, where the processing activities are related to:

- the offering of goods or services to data subjects in the EU, irrespective of whether payment is required by the data subject or
- the monitoring of the behavior of data subjects in the EU, in so far as their behavior takes place within the EU

➤ = goods, services, monitoring activities
● = establishment of controller / processor

WHAT DOES THIS MEAN FOR YOUR BUSINESS?

Activity Assessment: You should consider whether, pursuant to the GDPR, your company should carry out (either as controller or processor) an assessment of all its processing activities: (i) in the context of establishments in the EU, but also (ii) concerning those processing activities that target data subjects in the EU or monitoring their behavior, even when the controller or processor is not itself established in the EU.

4. DATA PROTECTION PRINCIPLES & ACCOUNTABILITY

Article 5 of the GDPR sets forth the major principles that have to be complied with when processing personal data.

- **Lawfulness, fairness and transparency:** *"Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject"*
- **Purpose limitation**: *"Personal data must be collected for **specified, explicit and legitimate purposes** and not further processed in a way incompatible with those purposes […]"*
- **Data minimization:** *"Personal data must be **adequate, relevant** and **limited to what is necessary** in relation to the purposes for which they are processed"*
- **Accuracy:** *"Personal data must be **accurate,** and, where necessary, be **kept up to date**." This includes an obligation to erase or rectify without delay any data which are inaccurate*
- **Storage limitation:** *"Personal data must be kept in a form which permits identification of data subjects **for no longer than is necessary** for the purposes for which the personal data are processed […]"*
- **Integrity and confidentiality:** *"Personal data must be processed in a way that ensures **appropriate security** of personal data, including **protection against unauthorized or unlawful processing** and against **accidental loss, destruction or damage,** using appropriate technical or organizational measures"*

WHAT DOES THIS MEAN FOR YOUR BUSINESS?

The controller is accountable for compliance, *i.e.,* the controller is *responsible for* and has to be able to *demonstrate compliance* with these principles. Several obligations under the GDPR (discussed below) are effectively tools that help the controller and processor to ensure that these principles are complied with and that this can be demonstrated.

5. LAWFULNESS OF PROCESSING

5.1 General

Processing of personal data is only legitimate, if one of the conditions for lawfulness listed in Article 6 of the GDPR can be invoked.

The processing of personal data is lawful **only** if and to the extent that at least one of the following applies:

- the data subject has given **consent** to the processing for one or more specific purposes
- the processing is **necessary for the performance of a contract** with the data subject or to take steps at the request of the data subject prior to entering into a contract
- the processing is **necessary for compliance with a legal obligation** to which the controller is subject
- the processing is **necessary to protect the vital interests** of the data subject or of another person
- the processing is necessary for the performance of a task carried out in the **public interes**t or in the exercise of official authority vested in the controller
- the processing is necessary for the purposes of the **legitimate interests of the controller or a third party**

With regard to **special categories of personal data,** processing is authorized in specific cases only. The most important of these are:

- where the data subject has given **explicit consent**
- where the processing is necessary to fulfil obligations/exercise rights under **employment/social security/social protection legislation**
- where the **vital interests** of a person must be protected
- where the data subject has **published these data elsewhere**
- where the processing is necessary to establishment, exercise or defense of **legal claims**

5.2 Requirements concerning consent

Under the GDPR, **consent** must be:

- given freely (genuine and free choice and possibility to refuse or withdraw consent without detriment – *not possible if there is clear imbalance between the data subject and the controller)*
- specific *(for a specific purpose)*
- "unambiguous" *(= requiring a "clear affirmative action")* and
- informed

When consent is given in the context of a written declaration which also concerns other matters, the request for consent must be:

- presented so as to be clearly distinguishable from the other matters
- in an intelligible and easily accessible form, using clear and plain language

In addition:

- it must be as easy to withdraw consent as to give it
- consent should be "explicit" in certain situations, *e.g.,* where special categories of personal data are concerned
- consent to processing in relation to information society services must be the consent of the holder of parental responsibility in the case of a data subject younger than 16 (this age can be lowered by Member States to an absolute minimum of 13 years)

WHAT DOES THIS MEAN FOR BUSINESSES?

- Existing contracts, terms & conditions, forms and other documents as well as websites have to be reviewed to **check the legal basis for the processing.** Is consent invoked, or is there another legal basis?
- If the legal basis for the processing is consent, it should be checked whether the way of obtaining the consent will result in **valid consent** and whether, for consent already obtained in the past, renewed consent should be obtained.
  - **Ticking boxes** on a website or the data subject using appropriate **browser settings** could still result in valid consent.
  - But: silence, pre-ticked boxes or inactivity **will no longer** constitute valid consent.
- If **legitimate interest** is the legal basis for the processing, this will have to be defined clearly.
- The **Article 29 Working Party** (new **European Data Protection Board**) will *i.a.,* consider whether its existing opinion on "consent" should be reviewed. Businesses should monitor these developments.

6. RIGHTS OF DATA SUBJECTS

The GDPR grants several rights to data subjects, which in turn are obligations for companies.

RIGHT	CONTENT	WHAT IS NEW?
Right to information	**Right to receive detailed information** about the processing when personal data is collected from the data subject or from other parties.	Information to be provided is **much more detailed** than before.
Right of access	Right to obtain from the controller confirmation as to whether personal data about the data subject is processed and, if so, **right to access to** personal data stored by the controller and to receive certain information.	More detailed information to be provided. Free of charge copy to be provided, also electronically when request is made by electronic means.
Right to rectification	**Right to ask rectification** of personal data which are inaccurate and to have incomplete personal data completed.	
Right to erasure ("right to be forgotten")	**Right to ask erasure** of personal data under certain conditions.	Conditions described in detail. Possibly an obligation to inform other controllers which are processing the personal data.
Right to restriction of processing	Right to **restrict** the processing (which means that only a limited use of the personal data is allowed),	Did not exist before.

	for instance, when the data subject contests the accuracy of the personal data.	
Right to data portability	Right to receive the personal data provided by the data subject, in a structured, commonly used and machine-readable format if the data had been provided on the basis of (i) consent or (ii) contract. Right to have the personal data transmitted directly from one controller to the other where technically feasible.	Did not exist before.
Right to object	Right to object to the processing based "on grounds relating to his or her particular situation", when processing was based on certain grounds (i.a., legitimate interest) or for certain purposes (statistical or research purposes) and absolute right in case of direct marketing.	No similar provision regarding statistical or research purposes in Directive.
Automated individual decision making, including profiling	Right "not to be subject to" a decision based solely on automated processing, including profiling, with certain exceptions such as explicit consent of Data subject.	Entirely new regime

The controller must provide information after requests under Articles 15 to 22 to the data subject without undue delay and at the latest within one month of receipt of the request. The information in principle has to be provided free of charge.

WHAT DOES THIS MEAN FOR BUSINESSES?

- All these rights in turn constitute **obligations** for businesses that are subject to the GDPR.
- Businesses have to make sure that **processes, technical measures and policies** are in place, which enable them to **adequately** (and in a timely fashion) **assess and handle** different types of **requests.**
- Businesses should make sure that employees are aware of the scope of these rights so **training** is required.
- Businesses should check their **existing contracts** and contract templates in order to ensure that:
  - current provisions in contracts with data subjects do not conflict with these rights
  - service providers are contractually required to ensure compliance with these rights
  - templates for future contracts with data subjects and third parties comply
- Businesses should check existing **data protection notices** and other documents communicated to data subjects when collecting personal data from these data subjects.
- Businesses should categorize their various processing operations, as some of these, such as **direct marketing,** processing on the basis of legitimate interest or for the performance of public tasks/official authority, will be subject to specific (information) obligations.

7. CONTROLLERS & PROCESSORS – GENERAL OBLIGATIONS

7.1 Controllers

Controllers are accountable for compliance with the principles contained in the GDPR. They should implement appropriate technical and organizational measures to ensure compliance with the GDPR when processing personal data, and they must also be able to demonstrate their compliance.

7.2 Data Protection by design and default

- **Data protection by design**
  - both at the time of the determination of the means for processing (development phase) and at the time of the processing itself, the controller has to implement appropriate technical and organizational measures which are designed to **implement the data protection principles**;
  - the controller should take into account the **state of the art** and the **cost of implementation,** as well as the **nature, scope, context** and **purposes** of the processing.
- **Data protection by default**
  - the controller has to implement appropriate technical and organizational measures to ensure that only personal data which are necessary for each specific purpose of the processing are processed by default;
  - this restriction applies to the amount of data collected, the extent of their processing, the period of storage and the data's accessibility.

7.3 Processors

- Controllers must only use processors who provide sufficient guarantees to implement appropriate technical and organizational measures to comply with the GDPR;
- Processing is to be governed by a contract that includes the items listed in Article 28 of the GDPR;
- There are specific obligations regarding the use of sub-processors;
- If processors infringe the GDPR by determining the means and purpose of processing, they will be considered a controller themselves.

7.4 Recordkeeping

- *"Each **controller** […] shall maintain a record of **processing activities** under its responsibility. This record shall contain the following information: […]".*
- *"Each **processor** […] shall maintain a **record of all categories of personal data processing activities** carried out on behalf of a controller, containing: […]".*

→ Required content of records is listed in the GDPR, but is different for controllers and processors.

→ Certain exceptions to the obligation exist.

WHAT DOES THIS MEAN FOR BUSINESSES?

- Processing activities by controllers and processors should be governed by a **written agreement,** including detailed terms as foreseen in the GDPR in order to limit the businesses' liability.
- **Obligations and potential liability** of businesses will **increase** under the GDPR (regardless of whether the company concerned is a controller or a processor).
- Businesses should:

  → *check the status of **policies, procedures, IT systems, security measures, available technology,** and **information sources** – are they sufficient to satisfy the requirements?*

  → *check the status of **staff's knowledge** about these requirements*

- If necessary, businesses should adapt **policies and procedures** and implement **appropriate technical and organizational measures** to prepare for compliance, including creating staff awareness via training.

8. DATA SECURITY AND DATA BREACH REPORTING

Giving the increased amount of personal data circulating across the globe in digital format, data security has become increasingly important for companies worldwide.

In addition, more and more legislations impose notification duties in case of data breach. The GDPR is not an exception.

8.1 Data security

Taking into account the **state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk** of varying likelihood and severity for the rights and freedoms of natural persons, the **controller and the processor** shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including *i.a.,*:

- **pseudonymization & encryption**
- the ability to **ensure** ongoing **confidentiality, integrity, availability** and **resilience** of systems and services processing personal data;
- the ability to **restore** the **availability and access to data** in a timely manner in the event of a physical or technical incident;
- **a process** for **regular testing, assessing and evaluating** the effectiveness of technical and organizational measures.

8.2 Data breach reporting

In case of a personal data breach, specific notification duties apply to both controllers and processors, and towards both the supervisory authorities and the data subjects concerned.

Notification obligations of controllers towards the supervisory authority:

- **Controllers** must **"without undue delay"** notify the competent supervisory authority

  Exception: not required when the breach is "unlikely" to result in risk for rights and freedoms of individuals

- Where feasible, this should be within **72 hours** of **becoming aware of the breach** *(if later, delay has to be **justified**)*

- **Content:**
  – Nature of data breach
  – Categories and approximate number of data subjects concerned
  – Categories and approximate number of data records concerned
  – Name and contact details of DPO or other contact person
  – Description of likely consequences
  – Description of measures taken or proposed to mitigate harm

Notification obligations of controllers towards the data subject:

- **Controllers** must **"without undue delay"** notify the data subject, if a personal data breach is
  *"likely to result in a **high risk** to the rights and freedoms of natural persons"*

- Content:
  – "**clear and plain** description of breach"
  – Contact details
  – Likely consequences
  – Measures taken

Notification obligations of processors:

The **processor** shall notify the **controller** "without undue delay" after having become aware of a data breach.

WHAT DOES THIS MEAN FOR BUSINESSES?

- Businesses should
  → check the status of **policies, procedures, IT systems, security measures, available technology, and information sources** – are they sufficient to deal with the requirements?
  → check the status of **staff's knowledge** about these requirements

- If necessary, businesses should adapt **policies and procedures** and implement **appropriate technical and organizational measures** to assure compliance, including creating staff awareness via training and data breach reporting processes.

- Check **agreements with third parties** (controllers / processors) regarding clauses relating to data security and breach handling.

9. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION

"High risk" operations require the **controller** to carry out particular **risk prevention activities:**

- The **"data protection impact assessment"** (Article 35) and
- a **"prior consultation"** of the supervisory authorities (Article 36).

A **"data protection impact assessment" (DPIA)** has to be carried out **in advance** for processing operations, which are likely to result in a **"high risk"** to the rights and freedom of natural persons *(in particular where the processing uses **new technologies**).* It is in particular required for:

- profiling
- processing of sensitive data on a large scale and
- systematic monitoring of publicly accessible areas (i.e., video surveillance)

A prior consultation **of the supervisory authorities has to be carried out prior to the processing** if a **DPIA** has indicated that:

- the processing would result in a **high risk** in the absence of measures taken by the controller to mitigate this risk

WHAT DOES THIS MEAN FOR YOUR BUSINESS?

- Businesses should implement procedures to assess whether specific processing could be classified as a "high risk" operation.
- Businesses should train staff in order to be aware of these obligations and should make the necessary staff available to perform the data protection impact assessments.
- Businesses should implement procedures for the performance of data protection impact assessments.

10. DATA PROTECTION OFFICERS

Controllers and processors have the **obligation** to appoint a **data protection officer** (DPO) if:

- the processing is carried out by a **public authority** or body, with the exception of courts acting in their judicial capacity
- the **core activities** of the controller or processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring of data subject on a large scale** or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data

The DPO has to be appointed on the basis of:

- professional qualities
- expert knowledge of data protection law and practices
- ability to fulfill (at least) the following tasks:
  – **inform and advise** the company and its employees
  – **monitor compliance** with the Regulation and other applicable law
  – **cooperate** and act as a contact point with the supervisory authority

In addition:

- the DPO can be either staff of the company or an independent service provider.
- groups of companies can appoint a single DPO, if easily reachable by each company.

WHAT DOES THIS MEAN FOR YOUR BUSINESS?

- The **core activities** of a business will determine whether or not it is **mandatory** to appoint a DPO
- If **not** mandatory, companies may consider the **voluntary** appointment of a DPO

Businesses should be aware that by appointing an external DPO, the responsibility for the compliance of a company with the Regulation will not be "outsourced"!

11. CODES OF CONDUCT & CERTIFICATIONS

- Codes of Conduct & Certifications constitute new, voluntary, compliance tools for businesses
- Under certain conditions, they can also be a possible **legal basis** for data transfers to third countries

11.1 Codes of Conduct

- Drafted by associations or bodies representing categories of businesses
- Content: application of the GDPR provisions for certain sectors
- The competent supervisory authority [1] will approve a Code of Conduct if it provides sufficient and appropriate safeguards – they can then be adhered to by companies subject to the GDPR.

→ **Important: International data transfers:**

– The European Commission can decide by way of an implementing act that Codes of Conduct, which have been approved by the EDPB, have **"general validity within the Union"**

→ *"codes of conduct with general validity" can be adhered to by businesses established in third countries as an* ***appropriate safeguard for international data transfers***

1. If the draft Code applies to several Member States, the EDPB must also be consulted before approval.
2. Certification bodies can be accredited if they have an appropriate level of expertise in data protection.

11.2 Certifications, seals, marks

- Issued by the competent supervisory authority or other accredited Certification bodies (Article 43)[2] and based on criteria approved by the supervisory authority or EDPB
- Can be adhered to for the purpose of demonstrating compliance with the GDPR
- Valid for a maximum period of 3 years; may be renewed or withdrawn

→ **Important: International Data Transfers:**

– Certifications issued on the basis of criteria approved by the EDPB "may result" in a common certification, the "European Data Protection Seal" (Article 42 (5)).

→ *this seal can be adhered to as* ***appropriate safeguard for international data transfers***

WHAT DOES THIS MEAN FOR YOUR BUSINESS?

- New ways for businesses to ensure and show their **compliance** with the GDPR
- New possibilities for the legitimation of **international data transfers**
- Businesses should monitor the publication of certifications and Codes of Conduct or set up their own draft Codes of Conduct together with trade associations

12. INTERNATIONAL DATA TRANSFERS

Data Transfers outside the European Economic Area (EEA) for purpose of further processing are still prohibited under the GDPR, unless *"the conditions [of the GDPR regarding data transfers, laid down in Chapter V] are complied with by the controller and processor […]".*

This requires <u>one</u> of the following conditions to be met:

1	**Adequacy decisions**[3]	= **Decision of the European Commission,** stating that the third country, territory or sector concerned ensures an **"adequate"** level of protection;	→ Data can be transferred to such a territory without further action or specific authorization.
2	**Appropriate Safeguards**		
	Standard Contractual Clauses	= **Model Clauses** issued by • the European Commission or **(NEW!)** the Supervisory Authorities (approved by the Commission)	→ if applied **without changes** to content, these clauses automatically legitimate transfers between the contract parties[4]
	Binding Corporate Rules	= Self-binding policy mechanism for **intra-group transfers** of multinational companies	→ Data can be transferred to **intra-group** companies
	NEW: EU Codes of Conduct **NEW : EU certification**	= Codes of conduct with general validity within the EU (approved by Commission) = certification mechanism based on criteria of the EDPB	→ Data can be transferred, if both EU and non-EU controller / processor adhere bindingly to the mechanism

3	**Specific Derogations**	
	Explicit consent	data subject has given <u>explicit</u> and <u>informed</u> consent to the transfer[5];
	Contract performance	= performance or conclusion of a <u>contract</u> with the data subject or a <u>contract</u> in the interest of the data subject;
	Public interest	= transfer for important reasons of public interest;
	Legal claims	transfer for establishment, exercise or defense of legal claims; = certification mechanism based on criteria of the EDPB
	Vital interests	= transfer in the vital interests of a data subject, who cannot consent
	Public source	= transfer from a public register

NEW: In very exceptional cases, the controller may also invoke his compelling legitimate interest as a new specific derogation.

EU-U.S. Privacy Shield

*The **EU-U.S. Privacy Shield,** a specific self-certification legitimation for data transfers from **Europe** to the **United States** on the basis of an **adequacy decision** of the European Commission, was formalized in the first half of 2016 and has been in force since August 1, 2016. U.S. companies can 'self-certify' with the U.S. Department of Justice and may then receive data from European companies without further legitimation or safeguards necessary.*

A similar system was already in place for several years under the 1995 Directive ("U.S.-EU Safe Harbor Framework"), but was invalidated in October 2015 by the European Court of Justice following the judgment in case C-362/14 ("Schrems").

3. Under the 1995 Directive, there are adequacy decisions for the following countries: Andorra, Argentina, Canada, Faroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, New Zealand, Switzerland, United States of America ('EU-U.S. Privacy Shield', for requirements *see below*), Eastern Republic of Uruguay. These will continue to apply under the GDPR, unless replaced, revoked or otherwise declared invalid.
4. Amended or ad-hoc contractual clauses can be used, if authorized by the competent supervisory authority.
5. Data Subject has to be informed of possible risks of such transfers due to absence of appropriate safeguards.

WHAT DOES THIS MEAN FOR BUSINESSES?

- Businesses should check if they have current data flows to outside the EEA
- If yes, businesses should check the legitimation mechanisms that are in place
  - – All transfers and purposes covered?
  - – Still valid?
  - – Appropriate?
- Determine data transfer mechanisms that suit your business best → for a first idea, have a look at our fact sheet 'International Data Transfers 2016'.

13. SUPERVISORY AUTHORITIES AND ONE STOP SHOP

- The GDPR introduces a "one stop shop" system: in principle, there will only be one competent national **supervisory authority** (SA) that is responsible for the supervision of EU Data Protection law.[6]
- Additionally, a **European Data Protection Board** (EDPB) will monitor, supervise and solve conflicts between national Supervisory Authorities and provide guidance.

13.1 Supervisory authorities

The GDPR foresees that Member States should establish one (or more)[7] independent **"supervisory authorities"** (SAs) and that, in general, each supervisory authority should be competent *"on the territory of its own Member State".*

13.2 Authority

The SAs will have the following tasks and powers[8]:

- **Investigative powers** – *i.a.,* audits, questionnaires, etc.
- **Corrective powers** – *i.a.,* orders, sanctions, fines. *(see point 15)*
- **Authorization and advisory powers** – *i.a.,* guidelines, adoption of Standard Data Protection Clauses, or certifications.

6. Usually, this is the authority in the Member State of the main establishment of a company in the EU.
7. If more than one supervisory authority is established in one Member State, a "main supervisory authority" will represent those authorities on an EU-level.
8. A full list of tasks can be found in Article 57 GDPR.

13.3 Cooperation and consistency – the “one stop shop”

- In general, in cases that concern trans-border processing, the SA of the main establishment of a company (“**Lead Authority**”) will take one single decision in cooperation with the other SAs concerned.
- If the **subject matter of a complaint** relates to a particular Member State, or substantially affects data subjects from that Member State, the **respective SA** should be competent. However, the Lead Authority may decide to handle the matter.
- SAs will also exchange information and provide mutual assistance.
- SAs are also entitled to conduct joint operations including joint investigations and joint enforcement measures (for details, see below).

14. EUROPEAN DATA PROTECTION BOARD

The European Data Protection Board will i.a.:

- **monitor** the adoption of measures taken by the competent supervisory authorities (SAs)
- act as a **dispute resolution body** in case of disputes between the SAs concerned
- issue **opinions, recommendations, best practices** and **guidance papers** for companies, authorities and/or individuals
- issue binding decisions, where necessary

15. CORRECTIVE POWERS, FINES, SANCTIONS

15.1 Corrective powers

The GDPR gives the supervisory authorities significant corrective powers, including the following :

- to order the controller / processor to **provide information**
- to order **access to personal data** held by the controller / processor
- to carry out **audits** and **investigations** (including on-site investigations)
- to issue **warnings, reprimands** or **orders** (for **rectification, erasure** or **destruction**)
- to place temporary or definite **processing bans**
- to **review** and (if necessary) **withdraw** certifications
- to **notify** controllers / processors of **alleged infringements**
- to execute significant **administrative fines**

The supervisory authorities can carry out these powers at their own initiative or following a complaint.

15.2 Administrative fines

The GDPR gives the supervisory authorities the power to impose administrative fines.

The fines imposed on controllers and/or processors based on infringements of the Regulation should be ***effective, proportionate and dissuasive*** in each individual case.

They apply in parallel to the right of data subjects to claim compensation and will be imposed in addition to or in place of other corrective measures:

Fine: the higher of…	Infringement of (examples) …
up to **€ 20,000,000** or **4%** of annual global turnover **(TO/yr)**	• **basic principles for processing** (including **consent**) • **data subjects rights** • rules on **international data transfers** • **national data protection law** • **non-compliance** with **orders** by supervisory authorities
up to **€ 10,000,000** or **2%** of **TO/yr**	• **accountability obligations** by controller / processor • **child consent, notification,** or **risk assessment** rules • **obligations** of **certification / Code of Conduct**

15.3 Additional sanctions under national law

- Member States are free to adopt other penalties for infringement of the GDPR, in particular for those infringements which are not subject to administrative fines under the GDPR.
- Member States law may also foresee criminal sanctions for companies and/ or their representatives.

These charges will depend on the respective Member State Law and might thus differ between the Member States.

WHAT DOES THIS MEAN FOR BUSINESSES?

- **Controllers** will still be primarily liable
  → *now, however, there are **significant administrational fines** for non-compliance and*
  → *possible **additional sanctions** under national law*

- **Processors** are now also directly liable for damages caused by infringements of the GDPR
  → *as a processor, it is no longer sufficient to "only" ensure compliance with contractual obligations towards the controller*
  → ***processors** also have to comply with the provisions of the law, to avoid **significant administrational fines** as well as possibly **additional sanctions** under national law*

→ **Regardless** of whether a business acts as a **controller or processor:** all businesses should execute an exhaustive compliance exercise in order to identify and minimize potential risks and to avoid possible **significant administrative fines** and **additional sanctions** under national law).

CROWELL & MORING LLP

Crowell & Moring is an international law firm with approximately 500 lawyers representing clients in litigation and arbitration, regulatory, and transactional matters. The firm is internationally recognized for its representation of Fortune 500 companies in high-stakes litigation, as well as its ongoing commitment to *pro bono* service and diversity. The firm has offices in Washington, D.C., New York, Los Angeles, San Francisco, Orange County, London and Brussels.

CONTACT

For further information please contact:

In our Brussels Office:

Frederik Van Remoortel
Senior Counsel
T. +32 2 282 18 44
E. fvanremoortel@crowell.com

Maarten Stassen
Senior Counsel
T. +32 2 214 28 37
E. mstassen@crowell.com

Emmanuel Plasschaert
Partner
T. +32 2 282 40 84
E. eplasschaert@crowell.com

Thomas De Meese
Partner
T. +32 2 282 18 42
E. tdemeese@crowell.com

In our Washington, D.C. Office:

Jeffrey Poston
Partner
T. +1 202 624 27 75
E. jposton@crowell.com

Jeane Thomas
Partner
T. +1 202 624 28 77
E. jthomas@crowell.com

Peter Miller
Senior Counsel
T. +1 202 624 25 06
E. pmiller@crowell.com

BRUSSELS

Rue Joseph Stevens 7
1000 Brussels
Belgium

P. +32 2 282 40 82
F. +32 2 230 63 99

CROWELL.COM