BeTECHSavvy
Securing Your Digital World

NATIONAL TRADING STANDARDS
Scams Team

The General Data Protection Regulation In More Detail

What You Need To Know

Incorporating
Umbrella Consulting

General Data Protection Regulation

Contents

Introduction 1

GDPR Key Changes 2 - 4

GDPR Key Change Analysis 4 - 10

1. **Application and Scope** 4 - 5
   - 1.1. Application
   - 1.2. Territorial Scope
   - 1.3. Exclusions
   - 1.4. Scope of Personal and Sensitive Data
2. **Principles** 5 - 7
   - 2.1 Lawful Processing and Further Processing
   - 2.2 Consent
   - 2.3 Parental Consent
   - 2.4 Legitimate Interests
   - 2.5 Privacy by Design and Privacy by Default
3. **Data Transfers** 7
   - 3.1 Cross-Border Data Transfer Rules
   - 3.2 Binding Corporate Rules
4. **Governance and security** 7 - 9
   - 4.1. Governance
   - 4.2. Information and Breach Notices
   - 4.3. Data Protection Officers
5. **Individual rights** 9
   - 5.1. The Right to Be Forgotten
   - 5.2. Subject Access Requests
   - 5.3. Data Portability
6. **Enforcement** 10
   - 6.1. One Stop Shop
   - 6.2. Sanctions

The right to data portability 10 - 13

Data Protection Officers 13 - 17

Lead Supervisory Authority 17 - 20

The EU General Data Protection Regulation ("GDPR") is probably to date one of the most lobbied legislation adopted by the EU since its creation. The Regulation introduces a single legal framework that applies across all EU member states. This change has been heralded as a major step towards a Digital Single Market and means that businesses will face a more consistent set of data protection compliance obligations from one EU Member State to the next.

The GDPR came into force on 25 May 2016 but it will only take effect for Member States by 2018, allowing for a two-year transition period. Significantly different from the old regulations, the GDPR will be directly applicable in all Member States, creating rights for all EU citizens to be relied upon without any need for implementing national legislation.

The Regulation ushers in many new concepts and approaches, likely to require organisation-wide adaptation for many businesses:

- Redesigning systems that process personal data;
- Renegotiating contracts with third party data processors; and
- Restructuring cross-border data transfer arrangements.

GDPR Key Changes

Key Issue	Changes introduced by the GDPR
Territorial Scope	Broader territorial scope will apply to: ▪ Data controllers and data processors established in EU that process personal data; and ▪ Data controllers and data processors not based in EU who target individuals who are in the EU
Data Processors	GDPR introduces direct statutory obligations for data processors, including: ▪ appointment of a Data Protection Officer; ▪ duty to notify the data controller without undue delay in case of a data security breach; and ▪ international data transfer obligations
Expanded definitions /new concepts	**Personal Data** – includes location data, online identifiers and technology identifiers **Pseudonymous Data** – defined as data that does not allow identification of individuals without additional information and is kept separate **Sensitive Data** – includes genetic data and biometric data **Profiling** - automated processing of personal data used to evaluate an individual's "personal aspects"

Consent	Consent must be either: ▪ unambiguous consent for general processing of personal data; or ▪ explicit consent for processing of sensitive personal data
Data subject rights	Existing rights are reinforced (access, rectification, deletion, objection to the processing) New rights: **erasure** (and right to be forgotten), **restriction** of the processing, data **portability**, right not to be subject to **data profiling**
Profiling	Automated decision making (including profiling) that either produces a **legal effect or significantly affects** individuals must be: ▪ authorised by law; or ▪ necessary to enter into or perform a contract with an individual; or based on individual's explicit consent
Minors	Consent must be obtained from parents when information society services are provided to minors below the age **of 16** (but cab be lowered to the age of 13)
Enforcement	DPAs now have **investigative** and **corrective** powers and they may impose fines of up to **EUR 20 million** or up to **4%** of worldwide annual turnover (whichever is higher)
Accountability	GDPR introduces new explicit principle of accountability – data controllers must ensure compliance with the general data processing principles
Records of processing activities	No more DPA registrations **But** controllers and processors must maintain internal records of all the data processing activities under their responsibility
Privacy by Design / Privacy by Default	GDPR introduces new concepts of '**privacy by design**' and '**privacy by default**' The controller must implement **appropriate technical and organizational measures** which are designed to integrate the necessary safeguards into the processing
Data Protection Impact Assessments	Data controller must carry out a **data protection impact assessment** prior to processing data where the processing is likely to result in a high risk for the rights / freedoms of individuals due to: ▪ the use of new technologies; ▪ the nature, scope, context and purposes of processing

Data breach notification	GDPR introduces an obligation to notify data breaches: **to the data protection authority within 72 hours; and to affected individuals without undue delay**
Data Protection Officer	Data controllers and processors must appoint a DPO in case of: ▪ regular and systematic processing of data subjects on a large scale; and ▪ when the core activities of the controller or the processor consist of processing on a **large scale** of sensitive data or data relating to criminal convictions and offences

GDPR Key Changes Analysis

1. Application And Scope

1.1 Application

The Regulation clarifies that it applies to controllers and processors alike. Under the old regime, the majority of its obligations were imposed on controllers. Allocation of responsibility between controllers and processors will therefore become more relevant.

It is also of note that despite being a regulation, the Regulation allows Member States to legislate in many areas. This will challenge the Regulation's objective of ensuring consistency.

1.2 Territorial Scope

The Regulation catches data controllers and processors outside the EU whose processing activities relate to the offering of goods or services (even if for free) to, or monitoring the behaviour (within the EU) of, EU data subjects. Therefore, a business outside the EU, which is targeting consumers in the EU, will be subject to the Regulation. This wider scope will likely make many more international businesses subject to the EU data protection regime.

1.3 Exclusions

The Regulation acknowledges that data protection rights are not absolute and provides certain exclusions. For example, the Regulation does not apply to the processing of personal data by a natural person as part of a "purely personal or household activity". This means that activities undertaken for social and domestic purposes including correspondence, social networking and other such online activities are not covered by the Regulation.

1.4 Scope of Personal and Sensitive Data

The Regulation establishes a single broad definition of personal data for the whole of the EU. What is fundamental to note is that the concept of identification will likely no longer be limited to the possibility of knowing the address, name, etc. of an individual, but rather will focus on the likelihood of "singling out" an individual whether directly or indirectly. The Regulation's recitals highlight that certain categories of online data may be personal, such as: online identifiers, device identifiers, cookie IDs and IP addresses.

"Special categories of data" (often referred to as "sensitive data") have also been expanded and now include genetic and biometric data. As was the case under the Directive, processing of such sensitive data is subject to tighter controls than other forms of personal data.

The Regulations introduces the concept of "pseudonymised data" (that is, key-coded or enhanced data). Pseudonymous data will still be treated as personal data, but subject to fewer restrictions on processing, if the risk of harm is low. It requires that the "key" necessary to identify data subjects from the coded data is kept separately, and is subject to technical and organisational security measures to prevent inadvertent re-identification of the coded data.

2. Principles

2.1 Lawful Processing and Further Processing

The Regulation sets out the conditions that must be satisfied for processing of personal data to be lawful. These conditions broadly replicate those in the Directive and are:
consent of the data subject (which is looked at in more detail at 3.2 below);

- necessary for compliance with a legal obligation;
- necessary to protect the vital interests of a data subject or another person where the data subject is no capable of giving consent;
- necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested
- in the controller; or
- necessary for the purposes of legitimate interests (which is looked at in more detail at 3.4 below).

The Regulation also establishes elements that must be taken into account to assess whether a new processing purpose is compatible with the purpose for which the data was initially collected. The following issues should be considered when determining whether there is compatibility:

- the nature of the data;
- the context in which the data was collected;
- any link between the original and proposed purposes;
- the possible implications of the proposed processing; and
- the presence of safeguards.

2.2 Consent

Obtaining consent before processing individuals' data will become more onerous under the Regulation. The definition of consent has been refined under the Regulation, which requires in relation to ordinary personal data, it to be "freely given, specific, informed and unambiguous" and will need to be shown by a clear affirmative action. It will not be able to be inferred from silence, pre-ticked boxes or inactivity.

One of the criticisms of the Directive was the varying level of consent required for different types of data processing. However, the Regulation perpetuates discrepancies, as it imposes the additional requirement that the processing of sensitive personal data can only be done with the subject's "explicit" consent.

The new regime is less permissive than what went before. If challenged, it will be up to an organisation to demonstrate that consent was given - underling the importance of an effective audit trail.

2.3 Parental Consent

The Regulation also introduces a requirement for parental consent where information society services are offered to children. This is one of areas though where there will not be harmonisation, as each Member State will be allowed under the Regulation to determine at which age (between 13 and 16) children no longer need parental consent. Many companies that operate across a number of Member States may elect to meet the highest standard across their operations.

2.4 Legitimate Interests

The Regulation's recitals give examples of processing that could be necessary for the legitimate interests of a controller, which include:

- processing for direct marketing purposes or preventing fraud;
- transmission of personal data within a group of undertakings for administrative purposes, including client and employee data
    I. processing for the purposes of ensuring information security; and
    II. reporting possible criminal acts or threats to public security.

2.5 Privacy by Design and Privacy by Default

The primacy of privacy in the Regulation is unquestionable and places a burden on businesses to implement two interrelated concepts: Privacy by Design and Privacy by Default. Privacy by Design requires that privacy should be embedded in the design of products and services from the outset and throughout their life cycle. Privacy by Default requires that privacy should be default setting for all products and a service, meaning that the collection, access, use and retention of data should be limited to that which is absolutely necessary for the specific purposes intended.

Businesses will have to take data protection requirements into account not only at the final stages of the product or service configuration, but from its very inception.

This will mean minimising the data collected and retained to what is absolutely necessary.
To achieve this, businesses will have to review their internal policies and procedures to ensure that privacy is built in as a consideration at every stage.

3. Data Transfers

3.1 Cross-border Data Transfer Rules

The Regulation will retain the cross-border data transfer rules of the Directive, so data may only be transferred out of the EU/EEA to countries which have been recognised as providing an adequate level of data protection, unless the transferor can rely on specific derogations or provides specific additional safeguards.

The existing list of countries which have previously been approved by the European Commission as providing an adequate level of data protection for data transfers will remain in force. For the time being, the approved countries are: Andorra, Argentina, Canada, Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Uruguay and New Zealand.

3.2 Binding Corporate Rules

Binding Corporate Rules ("BCRs") are agreements used to lawfully transfer personal data out of the European Economic Area (EEA). The Regulation expressly recognises BCRs as a means of legitimising intra-group international data transfers. To be valid they:

- still require data protection authority ("DPA") approval (but the approval process should become less onerous);
- must be legally binding and apply to and be enforced by every member of the group of companies engaged in a joint economic activity; and
- must confer enforceable rights on data subjects.

4. Governance And Security

4.1 Governance

The Regulation has at its heart the principle of "fair and transparent" processing and places onerous accountability obligations on data controllers to demonstrate compliance to a DPA if requested. The minimum measures include:

- maintaining extensive internal records on data protection activities;
- performing data protection impact assessments for high risk projects; and
- keeping "transparent and easily accessible" policies explaining to data subjects both how their personal data will be processed, what their individual rights are and how they may be exercised.

4.2 Information and Breach Notices

The principle of "fair and transparent" processing means that a controller must provide information to individuals about the processing of their data. The Regulation again expands an obligation that already applied under the Directive. The additional information that must now be provided includes the following:

- details of data transfers outside the EU;
- the retention period for the data; and
- that the individual can complain to a supervisory authority.

Another key change under the Regulation is the introduction of general data breach notification obligations. Subject to certain limited exceptions, a data controller must notify most data breaches to its DPA. Furthermore, in the event of serious data breaches (that result in a high risk, such as discrimination, identity theft or fraud, financial loss, breach of pseudonymity, damage to reputation, loss of confidentiality or any other significant economic or social disadvantage) the individuals concerned, must be notified. Notification must be done "without undue delay" and within 72 hours of awareness. If the data controller cannot do this, it will have to justify the delay to the DPA.

Security, from collection to secure deletion, should be a top priority for organisations when addressing data compliance. However, with cyber-attacks increasing, breaches are becoming more and more inevitable. Complying with the data breach reporting obligations imposes a further administrative burden. Businesses will need to act proactively to ensure that they react promptly in the event of a breach. This will involve drawing up data breach response plans (which will include designating specific roles and responsibilities, training employees, and preparing template notifications).

4.3 Data Protection Officers

In certain circumstances data controllers and processors must designate a Data Protection Officer (the "DPO"). A DPO is required if:

- the processing is carried out by a public authority;
- the core activities of the controller or processor consist of processing which, by its nature, scope or purpose, requires
  I. regular and systematic monitoring of data subjects on large scale; or
  II. the core activities consist of processing on a large scale of special categories of data.

The recitals to the Regulation clarify that:

- "special categories of data" comprise personal data relating to racial/ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual orientation and genetic or biometric data processed for unique identification purposes.
- "core activities" are its primary activities and do not relate to the processing of personal data as ancillary activities.

Therefore, companies handling employee data but not carrying out large scale monitoring of data subjects will not have to appoint a DPO despite employee data usually containing special categories of data.

A group of companies and certain groups of public authorities may appoint a single DPO (as long as accessibility to all is ensured). DPOs do not need to have a specific certification but will need to have sufficient expert knowledge. Their responsibilities will include:

- informing and advising the controller/processor, and its employees, of their obligations under the Regulation; and
- conducting risk assessments of the controller/processor's data processing operations.

5. Individual Rights

5.1 The Right to Be Forgotten

Data subjects will have rights to erasure of information (formerly known as the right to be forgotten) and be able to request that businesses delete their personal data without undue delay in certain circumstances (for example, when data is no longer necessary for the purpose for which it was collected).

When responding to such requests, data controllers will be required to perform a 'balancing act' against any competing rights to freedom of expression.
Also, exceptions apply to the erasure requirement where the controller may be able to demonstrate an overriding justification to maintain the processing of the data – for example, the need to retain records to comply with a legal obligation.

As a result of the expansion of data subjects' rights, businesses will need to devote additional time and resources administering these issues and ensuring that they are appropriately addressed. In particular, businesses should consider how they will give effect to the rights to erasure, as deletion of personal data can be complex.

5.2 Subject Access Requests

The Regulation also introduces changes to dealing with subject access requests. The general obligation that a request be accompanied by a payment will be removed. However, there will be additional grounds for refusing to comply with a request, and the possibility of charging a reasonable fee if the request is unfounded or excessive.

5.3 Data Portability

The Regulation introduces a new right to data portability - allowing data subjects to receive personal data, which they have provided to a controller, without hindrance and in a structured and commonly used machine-readable format. Moreover, the data subject is also entitled, where such a transfer is technically feasible and available, to direct one controller to transmit to another, the subject's personal data.

6. Enforcement

6.1 One Stop Shop

The Regulation provides a new system allowing businesses operating across Europe to answer to a single national DPA as its lead regulator for all compliance issues in the EU. The supervisory authority in question will be that in the country of the controller or processor's main point of establishment in the EU.

The principle should have the effect of reducing the administrative burden of compliance on businesses that currently need to interact with supervisory authorities in each Member State where they are operate. However, if the UK were to leave the EU, there is the possibility that businesses will not be able to use the Information Commissioner's Office (the "ICO") as lead regulator.

6.2 Sanctions

The Regulation exponentially increases the maximum fines. In the event of a serious breach of the Regulation, a fine could be the greater of EUR 20m or 4% of global annual revenue (in the most recent financial year).

Each national supervisory authority will be equipped with broad powers and will be able to enforce the sanctions referred to above. This is a major change from the current regulatory framework, where enforcement powers are inconsistent across the EU.

Businesses that had previously regarded non-compliance with EU data protection law as a low-risk issue will be forced to re-evaluate. These changes will significantly increase the risk associated with non-compliance and will mean that taking a view on data protection compliance is likely to become prohibitively expensive.

For each of the following three topics, the WP29 (Article 29 Working Party) has published both Guidelines and FAQs.

1. The right to data portability

The GDPR introduces a brand-new right to data portability and compliance will require organisations to make operational changes to their systems and databases in order to comply. The WP29 guidelines on the right to data portability provide guidance on the interpretation and the implementation of the new right to data portability. It aims at defining its scope and the conditions under which it applies irrespective of the legal basis of the data processing. The WP29 also recommends that data controllers and generally industry stakeholders and trade associations work together towards the creation of systems and tools as well as interoperable standards and formats so as to facilitate the response to data portability requests.

Key Issue	Changes introduced by the GDPR
Definition	Data subjects have the right to enjoy more control over their personal data, especially to reuse and manage it, or to switch between service providers. They "have the right: ▪ to receive the personal data concerning him or her, ▪ which he or she has provided to a controller, in a structured, commonly-used and machine-readable format and have the right ▪ to transmit those data to another controller without hindrance from the controller to which the data have been provided…"
Legal Basis	There is no general right of data portability. It only applies to data being processed with the data subject's consent or pursuant to the necessity to perform a contract. Other legal basis, such as processing that is required by law, or for the legitimate interest of the controller do not apply.
Interaction with Data Subject Access Request	There is no general right of data portability. It only applies to data being processed with the data subject's consent or pursuant to the necessity to perform a contract. Other legal basis, such as processing that is required by law, or for the legitimate interest of the controller do not apply.
Scope of the data	Data portability only applies to data processed by automated means and therefore excludes paper files. **In scope:** only personal data which concerns the data subject. It includes both the data provided by individuals and the personal data generated by a data subject's activity, including: ▪ through the use of the controller's services or device (such as data search history, traffic data, browsing behaviour or location data);

	▪ pseudonymous data clearly relating to a data subject; and ▪ personal data relating to several other data subjects. **Out of scope:** data inferred or derived by the data controller on the basis of the personal data provided by the data subject. Example: user profile or algorithmic results based on the data collected, credit score or analysis of the user's health. **Limitations** which cannot "in and of itself serve as the basis for a refusal to answer the portability request" include: ▪ the prohibition to transmit data which may adversely affect the rights and freedoms of a third party, unless the receiving data controller is pursuing a legitimate interest. ▪ Restrictions related to applicable trade secrets and intellectual property rights, such as database rights.
Format of the data	The many types of data that data subjects may request make it difficult to identify one format and it is recognised that there is no one appropriate format for providing this data, as long as it is "interoperable" for ease of sharing with other controllers. **Minimum standards** for the provision of the data by data controllers include: ▪ to provide for a high level of abstraction to allow for the data controller to remove information which is outside the scope of portability, such as passwords; ▪ to provide as much metadata as possible in order to preserve the precise meaning of the exchanged information; and ▪ to securely deliver information to the correct individual and ensure that the information is transmitted and stored as securely as possible.
Specific technical obligations for Data Controllers	Data controllers are required to provide a range of tools and technical measures to facilitate data subject's requests including the provision of: ▪ a process for acknowledging receipt of requests, to confirm the identity of the data subject and respond to the requests without undue delay; ▪ a direct download option from the controller's website and an option to automatically transmit data to another data controller. Example: providing an application programming interface (API) may help.
General obligations for Data Controllers	**Inform** data subjects regarding the availability of the new right to portability "in a concise, transparent, intelligible, and easily accessible form, using clear and plain language" (including before any account closure).

	Respond to requests without undue delay, and in any event within one month of the initial request. **Identify** and implement an authentication procedure so as to verify the identity of the data subject exercising the request. **Time** extension in the event that the data requested may prove difficult to transfer, for up to three months from the relevant supervisory authority. **Implement all security** and authentication measures necessary to ensure the secure transmission and storage of the personal data of data subjects (e.g., by use of encryption) to the right destination (e.g., by use of additional authentication information). Because of the risk that data subjects might request or their data but then fail to keep it secure, controllers responding to portability requests should recommend appropriate format(s) and encryption measures to help the data subject maintain security. **Interoperability** so that personal data may be accessed by most other data controllers in a common format.
Interaction with Data Retention and Erasure	Data portability does not impact data retention obligations. Organisations are not required to retain personal data in the event that a data subject may choose to exercise this right. Similarly, a data subject's data portability request does translate by itself into a request to delete that data subject's personal data. Data retention and Data portability requirements apply in parallel.

2. Data Protection Officers

Although the role of DPOs is already required by some Member States' national laws (such as Germany and Sweden), it is not currently mandatory under EU Data Protection Law, to appoint a DPO. The GDPR will introduce significant new obligations which will require many organisations to appoint DPOs. The WP29 recognise the importance of DPOs") as being "at the heart" and at the forefront of the organisation's obligation to comply with the requirements of the GDPR. The new Guidelines on DPOs provide businesses with useful information on the roles and responsibilities of DPOs.

Key Issues	Changes introduced by the GDPR
Definition	A DPO is a person (either an employee or an external consultant) who is given formal responsibility for data protection compliance within an organisation.
Legal Basis	Article 37(1) of the GDPR requires the mandatory designation of a DPO in the following three cases:

	▪ the relevant data processing activity is carried out by a public authority or body; ▪ the data controller or processor's core activities involve regular and systematic monitoring of data subjects, on a large scale; or ▪ the data controller or processor's core activities of the relevant business involve processing of special categories of data, or data relating to criminal convictions and offences, on a large scale. ▪ The Guidelines provide a more detailed explanation of these concepts, enabling businesses to better understand their compliance obligations.
Rules on DPO Appointments	The guidelines clarify key concepts used in the GDPR: **Core activities** are described as those activities that "can be considered as the key operations necessary to achieve the controller's or processor's goals". Conversely, "core activity" may not include standard IT support or employee compensation which should be considered "ancillary functions" rather than a company's "core activity." **Large scale** of special categories of personal data (referred in many cases as "sensitive data") consists of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." Such qualification may depend on a number of factors including: ▪ The number of data subjects concerned, either as a specific number or as a proportion of the relevant population. ▪ The volume of data and/or the range of different data items being ▪ processed. ▪ The duration or permanence, of the data processing activity. ▪ The geographical extent of the processing activity. Examples of "large scale" sensitive data processing include hospital's processing of patient data, whereas examples of non-"large scale" processing include an individual lawyer's processing of criminal convictions.
Rules on DPO's Appointment (continued)	**Regular and Systematic Monitoring** include "all forms of profiling and tracking on the internet, including for purposes of behavioural advertising". Clearly, behavioural advertising agencies will be required to appoint a DPO. Other examples include: the operation of a telecommunications network; profiling and scoring for the purposes of risk assessment; location tracking; fitness and health data via wearable devices; and connected devices.

	Organisations are required to carry out an internal analysis so as to determine whether they require a DPO. It is left to the discretionary decision of the organisations that may not require a DPO to designate a DPO on a voluntary basis. In such case, all GDPR requirements on DPO's position and tasks shall become mandatory. However, they may also appoint other staff to perform tasks relating to data protection compliance. It is important for such staff not to be referred as 'DPOs' so as to or avoid any amalgamation with the status of a DPO appointed voluntarily.
DPO requirements	The requirements that designated DPOs are expected to fulfil are as follows: **Accessibility** – a group of undertakings can appoint a single DPO, as long as he or she is personally available to efficiently communicate with data subjects, supervisory authorities and internally within the organisation (including in the language or languages of the supervisory authorities or data subjects concerned). A single DPO must be able to perform their tasks efficiently despite being responsible for several undertakings. **Expertise** - the DPO must have a level of expertise that is commensurate to the sensitivity, complexity and amount of data processed by the relevant organisation (i.e. importance of the transfers outside EEA); a DPO can be appointed on a part-time basis, alongside other duties,; provided that those other duties do not give rise to conflicts of interest and as long as the DPO is given sufficient time to fulfil their duties as a DPO. An external DPO, or DPO team may be appointed, provided that the DPO must be able to fulfil its / their tasks, they must be independent, and they must be afforded sufficient protection (for example, from unfair termination of a service contract). **Professional qualities** - the DPO should have expertise in national and European data protection law, including an in-depth knowledge of the GDPR. DPOs appointed for public authorities should have an excellent knowledge of the administrative procedures of their organisation, while DPOs operating in the private sector must also have a good knowledge of the industry within which they are active. **Ability to fulfil task** - the DPO should demonstrate integrity and high professional ethics and, as a primary concern, enable compliance with the GDPR

Role of the DPO	Organisations are required to seek and consider the DPO's advice at all times and from the earliest stage possible, on all issues relating to the protection of personal data. As part of the organisations' standard governance rules, the DPO will need to be appropriately informed on all relevant associated matters; invited to participate regularly in meetings of senior and middle management; and required to attend whenever projects have data protection implications; and promptly consulted once a data breach or other incident has occurred. DPOs' tasks may include: ▪ monitoring the organisation's compliance with the GDPR, and advising on data protection issues; ▪ carrying out data protection impact assessments. Where high-risk processing is contemplated, the business should actively seek advice from the DPO on conducting a DPIA. The DPO is expected to take a risk-based approach, and prioritising the assessment of high-risk processing activities; and ▪ other data protection related tasks such as maintaining the record of processing operations.
Protection for DPO's	In order to protect DPOs autonomous and independent status within an organisation, they benefit from protections against unfair dismissal or termination based on the performance of their role. In some EU Member States, a DPO who has the status of an employee may also benefit from the protections afforded by local employment law. In case of disagreement with the DPO, the organisation will need to document its reasons why the DPO's advice is not being followed. Due to the high level of responsibilities given to DPOs, they cannot be terminated or otherwise penalised (e.g. demotion, denial of promotion, etc.) for providing advice within the scope of their responsibilities albeit contrary to the organisation's view. The same protections apply should an organisation decide to appoint an external DPO (e.g., no unfair termination of the service contract for activities as DPO).

3. Lead Supervisory Authority

The WP29 provides guidelines for identifying a controller or processor's lead supervisory authority. This set of guidelines is especially helpful for those companies that carry out cross-border processing of personal data, defined as data processing that takes place when a controller or processor has establishments in multiple Member States, or where the controller or processor is established in a single Member State but the processing "substantially affects or is likely to substantially affect" data subjects in multiple Member States.

These rules will determine which DPA takes the lead in any enforcement action with a cross border dimension. These GDPR rules aim to simplify and improve the relationship of multinational organisations established in various Member States with the relevant DPAs as opposed to being subject to multiple DPAs in each jurisdiction.

This set of guidelines recognizes that the designation of a lead supervisory authority necessarily is a very fact-specific inquiry. Although it provides some generalized advice, it also includes illustrative examples and factors for companies to consider in making the determination for themselves. To that end, the guidelines also include an annex meant to guide companies going through the designation process. Some of the more general points are described below.

In these situations, the GDPR allows controllers and processors to designate a single local authority to act as the "lead supervisory authority" which role is to oversee their operations and compliance with the law. This has become known as the "one stop shop" approach.

Key Issues	Changes introduced by the GDPR
The "one-stop shop mechanism	This is one of the central pillars of the GDPR. It is also called "consistency mechanism" It is meant to help multinational organisations deal with a single supervisory authority, in spite of having a number of establishments across the EU Member States. This mechanism is available to both controllers and processors carrying out the 'cross-border processing' of personal data in the event that either may have: ▪ establishments in two or more EU Member States and the processing of personal data takes place in the context of their activities in those establishments; or ▪ only carries out data processing activities in the context of its establishment in one EU Member State, but the activity substantially affects, or is likely to substantially affect data subjects in more than one EU Member State.
Identifying the Lead Supervisory Authority	The designation of a lead supervisory authority is driven by very fact-specific parameters. For **controllers** engaged in cross-border data processing, the lead supervisory authority will be the supervisory authority in the Member State in which the controller has its "main establishment" or 'single establishment'. The definition of the main establishment refers to the place of the "central administration" of the controller in the EU and where the controller makes "decisions on the purposes and means of the processing." However, if data protection decision- making occurs in different EU Member States, several detailed examples explain how to determine in which EU jurisdiction is the "main establishment."

	For **processors** with establishments in more than one EU Member State, they may also benefit from the 'one-stop-shop mechanism'. The processor's main establishment will be the place of the central administration of the processor in the EU or, if there is no central administration in the EU, the establishment in the EU where the main processing takes place.
Identifying the Lead Supervisory Authority (continued)	For **Groups of undertakings**, the lead authority is likely to be the authority in the Member State where the undertaking with overall control is established – this is likely to be the parent undertaking or 'central administration'. Where groups of companies have more complex decision-making processes, with different establishments having independent decision-making powers, the lead authority will be in the Member State where the exercise of management activities that determine the main decisions relating to personal data takes place. In cases involving both controller and processor, the competent lead supervisory authority will be the lead supervisory authority for the controller.
Role of the Lead Supervisory Authority	The lead supervisory authority will have primary responsibility for dealing with cross-border processing activities and will coordinate investigations into breaches by the controller or processor.
Companies Not Established in the EU	he one-stop shop system is not available to an organisation which does not have any establishment in the EU. Such organisation will be subject to the supervisory authorities in each EU Member State in which it operates. The fact that an organisation may have appointed a single representative in one Member State does not mean that person may qualify as a "main establishment" for one- stop shop purposes. This requirement may weigh in heavily on SMEs.
Prohibition of "Forum shopping"	Controller and processors are not allowed to do any 'forum shopping' choosing a supervisory authority by claiming they have their main establishment in such Member State when the management activity is actually exercised in another Member State. Supervisory authorities may challenge the designation by an organisation of a lead authority and ultimately decision may be referred to the European Data Protection Board (EDPB) to objectively define which authority is in fact the 'lead'.
Concerned authorities	When the one-stop-shop mechanism is available, the lead supervisory authority will closely involve and co-ordinate other 'concerned' authorities in its enforcement of the GDPR.

	Lead authorities must consult with 'concerned' supervisory authorities through the cooperation procedures set out in the GDPR. A supervisory authority may be 'concerned': ▪ if the controller or processor has an establishment in that Member State, and ▪ if data subjects residing in that Member State will be substantially affected by processing, or ▪ if a complaint has been lodged with that Member State. Concerned authorities will therefore have competence to oversee how a case is dealt with when either of these criteria apply. A lead authority may decide not to handle a case if it would be more appropriate for the concerned supervisory authority who informed the lead authority of the case to do so.
Data Subjects rights	Data subjects may lodge a complaint with any supervisory authority. However, such supervisory authority will then be required to inform the lead supervisory authority, which will in turn determine whether it will handle the complaint. If the lead supervisory authority decides that it does not have "jurisdiction" to handle the complaint itself, the supervisory authority to whom the complaint was made will handle it.
The European Data Protection Board ("EDPB")	The European Data Protection Board ("EDPB") is a body established under the GDPR, which will succeed to the WP29. **Concerned authorities** Likewise, it will include the head or representative of one supervisory authority from each Member State and of the European Data Protection Supervisor ("EDPS"). The European Commission also has a non-voting right to participate on the Board. The EDPB has a lengthy list of tasks. Whereas the WP29, was essentially an advisory committee producing recommendations and opinions, the EDPB will have a more formal and binding role relating to the enforcement of data protection law. The primary obligation of the EDPB is to ensure the consistent application of the GDPR by the EU Member States.