

# GDPR Q&A | Twenty-one Questions and Answers to assist companies in complying with the General Data Protection Regulation

## | INTRODUCTION

Personal data has become one of the most critical assets for businesses today. Whether it relates to employees, customers, users, patients, targets or your contacts, personal data is found in all departments of a company. With advances in technology, companies are finding novel ways of using this data. However, the proliferation of data also challenges the rights of the data subjects. Therefore, these individuals have to be given some control and information over the use of their personal data. They also have to be protected against the potential harm that they could suffer from the illicit or unwanted use of information that relates to them.

The Charter of Fundamental Rights of the European Union establishes that everyone has the right to the protection of personal data concerning him or her. In the EU, the new "General Data Protection Regulation" (**GDPR**) further elaborates on the rights and obligations when processing personal data.

The GDPR contains significant new obligations, when compared to the regime applicable under Directive 95/46/EC, and raises the stakes for data protection compliance in terms of responsibility and liability. The "*accountability principle*" makes companies responsible for implementing data protection policies as part of their daily operations and activities (see, Question 6). The GDPR also imposes significant fines for breaches of its provisions. The fines could amount to as much as EUR 20 million or 4% of the company's worldwide annual turnover (whichever is higher). Moreover, data subjects are encouraged to actively protect their rights and seek redress before supervisory authorities or national courts.

The questions below are those which Van Bael & Bellis' data protection team have found to be the most commonly asked by clients actively working to comply with the GDPR. The responses are not exhaustive and companies doing business in Europe should seek legal advice if they feel that they may be affected by this highly complex and considerably far-reaching legislation.

This document should not be construed as legal advice on any specific facts or circumstances. The content is intended for general informational purposes only. Readers should consult attorneys at the firm concerning any specific legal questions or the relevance of the subjects discussed herein to particular factual circumstances.

# GDPR Q&A | Twenty-one Questions and Answers to assist companies in complying with the General Data Protection Regulation

## | CONTENTS

1.	We do not target customers using personal data – is the GDPR still relevant to us?	p. 3
2.	Does the GDPR also apply when personal data are processed outside the EU?	p. 3
3.	Does the GDPR allow flexibility in its application?	p. 3
4.	I heard that we no longer need to file a notification for each processing? Is that true?	p. 4
5.	Do we need to certify compliance by certification bodies?	p. 4
6.	What does "accountability" mean in practice?	p. 5
7.	Is it still possible to rely on implicit consent?	p. 5
8.	Should we update the information given to data subjects?	p. 6
9.	How can data subjects ask to "be forgotten"?	p. 7
10.	Can data subjects request a copy of their personal data or transfer these data to another service (data portability)?	p. 7
11.	Does the GDPR restrict profiling of data subjects?	p. 7
12.	Does the GDPR also apply if I use pseudonymous or encoded data?	p. 8
13.	What does a controller need to do when it relies on data processors?	p. 9
14.	My company processes personal data on behalf of other companies, what does the GDPR mean for us as a processor?	p. 9
15.	Data breach notification: what to do when your personal data has been breached?	p. 10
16.	I was informed that as a director of a company I have to appoint a data protection officer (DPO). Is this true for all companies?	p. 11
17.	My group of companies operates in different parts of the world. Can I still transfer personal data to countries outside the EU/EEA?	p. 11
18.	To which supervisory authority should I report?	p. 12
19.	Does the Regulation provide full harmonisation or are there differences between Member States?	p. 12
20.	How do I ensure that my organisation is GDPR compliant?	p. 13
21.	What is the risk if my organisation fails to comply with data protection rules?	p. 13

This document should not be construed as legal advice on any specific facts or circumstances. The content is intended for general informational purposes only. Readers should consult attorneys at the firm concerning any specific legal questions or the relevance of the subjects discussed herein to particular factual circumstances.

## 1 | WE DO NOT TARGET CUSTOMERS USING PERSONAL DATA – IS THE GDPR STILL RELEVANT TO US?

Data protection regulation is present in all aspects of our lives and businesses. The GDPR is still relevant to you even if your business does not specifically target customers using personal data. In fact, all human resource records are personal data. Do you have any security or access systems? They too produce personal data, as well as IT systems, company phones, CCTV, contact databases, newsletters, online registrations, etc. Personal data are literally everywhere in today's companies. Moreover, if these personal data are being handled by third parties, such as payroll or IT companies, then it is necessary to have

a contract with these parties, foreseeing specific obligations in terms of data protection. Are you transferring data overseas? If so, then precautionary measures need to be taken to ensure an adequate level of protection for the personal data transferred.

These are but a few of the numerous obligations that arise out of data protection regulation. Based on the broad definition of personal data as any information relating to an identified or identifiable individual, it is safe to assume that, effectively, every company is affected by the GDPR.

## 2 | DOES THE GDPR ALSO APPLY WHEN PERSONAL DATA ARE PROCESSED OUTSIDE THE EU?

The territorial scope of the EU data protection rules has been extended under the GDPR, which also applies to non-EU companies that target EU residents.

For processors or controllers established in the EU, the GDPR applies to all processing of personal data in the context of the activities of EU establishments.

Controllers or processors that are not established in the EU may also be subject to the GDPR when they offer goods or services in the EU or monitor data subjects' behaviour taking place in the EU. When this is the case, a representative in the EU needs to be appointed.

## 3 | DOES THE GDPR ALLOW FLEXIBILITY IN ITS APPLICATION?

The GDPR describes the responsibility of the controller as allowing certain flexibility (the so-called risk-based approach). The controller is required to implement "appropriate" technical and organisational measures to ensure and be able to demonstrate compliance.

To determine what is deemed to be "appropriate", the controller must take account of the nature, scope, context and purposes of the processing as well as the

risks, and their severity, in relation to the rights and freedoms of individuals.

In other words, strict compliance measures are required for high-risk processing, whereas lower standards can be applied to operations that are unlikely to pose any risk. For instance, controllers may be exempt from the obligation to notify data breaches if the risk is very low and data protection impact assessments are only required for high-risk operations.

## 4 | I HEARD THAT WE NO LONGER NEED TO FILE A NOTIFICATION FOR EACH PROCESSING? IS THAT TRUE?

The general obligation to notify data processing activities provided for by Directive 95/46 has been abolished under the GDPR. However, prior consultation of the supervisory authority is necessary in specific cases where it follows from a data protection impact assessment that the processing would result in a high risk if the controller fails to take measures to mitigate that risk. Prior authorization from the supervisory authority may also be necessary when transferring personal data to third countries.

Instead of systematically notifying public authorities, the GDPR obliges companies to maintain up-to-date internal records on their processing of personal data, containing similar information to the current notifications.

Needless to say, the obligation to keep up-to-date internal records places a significant burden on controllers. However, and subject to certain conditions, SMEs are exempt from this obligation.

The obligation to keep and update internal records must be read as part of the GDPR's aim to ensure that companies install a data protection culture in their everyday operations. In the same vein, the "accountability" requirement obliges data controllers to demonstrate compliance with the data protection principles (see, Question 6).

## 5 | DO WE NEED TO CERTIFY COMPLIANCE BY CERTIFICATION BODIES?

There is no legal requirement for companies to have their compliance practices certified by certification bodies. Nonetheless, under the *accountability* principle (see, Question 6), controllers are now explicitly required to "demonstrate compliance" with the data protection principles under the GDPR. The GDPR refers to tools to help demonstrate compliance, such as codes of conduct, seals or certification.

Codes of conduct will be developed by industry and approved by supervisory authorities, whereas seals or certifications will be granted by certification bodies, supervisory authorities or the European Data Protection Supervisor (*EDPS*).

Supervisory authorities shall encourage the development of codes to take account of the specific features of particular industries and sectors. Where a supervisory authority approves a code, adherence can be relied upon by organisations to demonstrate compliance with other aspects of the GDPR. Controllers and processors that adhere to either an approved code of conduct or an approved certification mechanism may therefore use these tools to demonstrate compliance with the GDPR standards or specific obligations thereunder, such as the adoption of appropriate security measures.

Data protection seals and certification marks allow controllers to show their compliance to data subjects in a way which is objectively verifiable. For data processors, certification may be a means to show the controller that they are a trustworthy partner.

*The GDPR introduces the principle of 'accountability' as a key principle for EU data protection.*

## 6 | WHAT DOES "ACCOUNTABILITY" MEAN IN PRACTICE?

The GDPR introduces the principle of "*accountability*" as a key principle for EU data protection. This requires controllers to implement a compliance program that is able to monitor compliance throughout the organisation and demonstrate to supervisory authorities and to data subjects that it is treating personal data in compliance with the GDPR.

By specifically referring to *accountability*, the GDPR shifts the manner in which organisations and supervisory authorities approach data protection compliance, encouraging data controllers to do so in a more proactive (and effective) manner.

Actions to comply with the principle of *accountability* include (i) implementing internal and external policies and compliance procedures; (ii) keeping detailed and up-to-date documentation on the processing of personal data (see, Question 4); (iii) carrying out data protection impact assessments for high risk processing operations; (iv) applying data protection by design and by default; (v) ensuring security and confidentiality by all internal and external parties involved in data processing operations; (vi) carrying out audits and certification (see, Question 5); (vii) and appointing a Data Protection Officer (see, Question 16). Depending on the situation, these actions are obligatory under the GDPR.

## 7 | IS IT STILL POSSIBLE TO RELY ON IMPLICIT CONSENT?

Consent remains a lawful basis to process personal data under the GDPR. However, the definition of consent is significantly restricted. While Directive 95/46/EC allowed controllers to sometimes rely on 'opt-out' and implicit consent (as long as this action or inaction was "unambiguous"), the GDPR requires the data subject to show agreement by a statement or a "clear affirmative action". In addition, consent must be "freely given, specific and informed" and the controller must be able to demonstrate that consent was given. Where, under Directive 95/46/EC, processing was based on consent, it is not necessary for the data subject to give its consent again if the way in which the consent was given is in line with the conditions of the GDPR.

In order to be "freely given", there must be a genuine and free choice and the data subject must be able to withdraw or refuse consent without detriment. The recitals of the GDPR introduce a presumption that consent is not freely given if there is an imbalance of power between the data subject and the controller, especially where the controller is a public authority or an employer.

*Consent remains a lawful basis to transfer personal data under the GDPR. However, the definition of consent is significantly restricted.*

In any case, the performance of a contract may not be made conditional on the consent to processing personal data that is not necessary to perform that contract.

Controllers must inform the data subjects of their right to withdraw consent before consent is actually given. The GDPR also allows data subjects to withdraw consent at any time, making it "as easy to withdraw consent as to give it".

Consent must be specific to each data processing operation, and "clearly distinguishable" from any other matters.

This means that if the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Finally, in order for consent to be "informed", the controller must provide certain information such as

its identity, the purpose of the processing activity and the rights of the data subject over his or her data. Once again, clear and plain language should be used in this regard.

There are some cases that require specific consent. The processing of sensitive categories of data requires 'explicit' consent. Or, in the case of minors (below 16 years of age), parental consent is required. If provided for by national law, a lower age than 16 is acceptable, but not lower than 13.

## 8 | SHOULD WE UPDATE THE INFORMATION GIVEN TO DATA SUBJECTS?


The notice that is given to data subjects in privacy policies, contracts, terms and conditions, etc. allows controllers to demonstrate compliance to data subjects. Controllers have to review their contact points, such as the various interfaces where a company provides information to data subjects, to ensure that the notice complies with the requirements of the GDPR.

The list of information that needs to be given to data subjects is expanded under the GDPR. Controllers must for instance also disclose for how long data will be stored, and inform data subjects of their rights to withdraw consent (if applicable), their right to request

access, rectification or erasure and restriction of processing, as well as their right to lodge a complaint with the supervisory authority and the contact details of the data protection officer (DPO) (if any). If the processing operation is based on the controller's legitimate interest, the controller must also explain to the data subject for which legitimate interest it will use the data, and if the data are transferred to a third country which is not recognised as giving adequate protection through its national laws, the data subject must be informed about the safeguards that the controller has put in place to protect the personal data. When the data have not been obtained directly from the data subject, the controller must explain how it obtained the personal data.

Vague or legalistic language is banned under the GDPR. Information must be intelligible and easily accessible, using clear and plain language that is tailored to the appropriate audience. The GDPR also permits the use of standardised icons to inform data subjects.

The obligation to inform data subjects applies irrespective of the legal basis of the processing activity. Even if the processing does not rely on the consent of the data subject, but instead is necessary to perform a contract or to comply with a legal obligation, the controller still has to inform the data subject how it processes his or her personal data (unless the provision of such information would be impossible or involve a disproportionate effort).



*Vague or legalistic  
language is banned  
under the GDPR.*

## 9 | HOW CAN DATA SUBJECTS ASK TO "BE FORGOTTEN"?

The right to be forgotten or the "right to erasure" allows individuals to request the deletion of their personal data and, where the controller has published the data, to require other controllers to do the same.

The right to "be forgotten" applies to all controllers (and not only to online search engines). Under the GDPR, controllers must erase data "without undue delay" if the data is no longer needed, the data subject objects to processing, the data subject withdraws his/her consent when that consent is the legal basis used for processing or the processing is unlawful.

In addition, where the data controller made the data subject's personal data publicly available, it must take reasonable steps to inform third party controllers who are processing the data that the data subject requested erasure of the data.

The right to be forgotten must, however, be balanced against freedom of expression, public health interests, scientific and historical research, and the exercise or defence of legal claims.

## 10 | CAN DATA SUBJECTS REQUEST A COPY OF THEIR PERSONAL DATA OR TRANSFER THESE DATA TO ANOTHER SERVICE (DATA PORTABILITY)?

In addition to the existing right to access personal data, the GDPR introduces a new right to obtain a copy of the data and the right of "data portability". The right to data portability requires controllers to provide personal data to the data subject in a commonly used format and to transfer that data to another controller at the data subject's request.

The GDPR provides that, where controllers process personal data "through automated means" data subjects have the right to transfer that data to any other controller.

In fact, a controller may even be required to hand data over to a competitor. Nonetheless, data portability does not oblige controllers to implement processing systems that are technically compatible with others' systems.

Importantly, the right to data portability only applies when processing was originally based on the user's consent or on the necessity to perform a contract, and does not apply to processing based on a public interest or the controller's legitimate interests. Further, it only relates to personal data provided by the data subject and not to "inferred data" or "derived" data created by the data controller.

## 11 | DOES THE GDPR RESTRICT PROFILING OF DATA SUBJECTS?

The GDPR defines profiling as "any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects relating to a natural person".

This includes tracking with the intention to predict the subject's behaviour and preferences, a technique which is often used in the online environment.

Data controllers must inform individuals specifically about the existence of profiling. Data subjects do not necessarily have the right to object to profiling itself, but they can object to being subject to decisions based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her (unless it is necessary for the performance of a contract, authorised by national law, or based on the explicit consent of the data subject). In other words, a decision which can have significant effects for the data subjects, such as being given a job or a bank credit, should not be based on an automated process or profile, without human intervention.

The GDPR also prohibits profiling decisions based on sensitive personal data, unless the data subject has given his/her explicit consent or where such profiling is necessary for reasons of public interest. Where automated decisions are permitted, the responsible company will need to provide additional information to data subjects on how the decision-making process works, and allow data subjects to demand human intervention reviewing the decisions that affect them.

Systemic use of profiling requires companies to carry out a prior data protection impact assessment.

## 12 | DOES THE GDPR ALSO APPLY IF I USE PSEUDONYMOUS OR ENCODED DATA?

Along with the concepts of personal and anonymous data, the GDPR introduces the novel concept of "pseudonymisation" into European data protection law.

The GDPR defines "pseudonymisation" as a privacy-enhancing technique through which personal data is processed in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.

In order to pseudonymise data, the additional information must be kept separate and must be subject to technical and organisational measures to ensure non-attribution to an identified or identifiable person.

Pseudonymous data is not exempted from the scope of the GDPR and thus remains subject to the data protection requirements. Nevertheless, due to its lower level of privacy intrusion, the GDPR foresees a less stringent regime for the processing of pseudonymous data, creating incentives for data controllers to use this technique.



Amongst others, the GDPR provides that pseudonymisation may facilitate processing personal data beyond the original collection purposes; may constitute an important safeguard for processing personal data for scientific, historical and statistical purposes; and may facilitate compliance with the GDPR's data security and data by design requirements.



## 13 | WHAT DOES A CONTROLLER NEED TO DO WHEN IT RELIES ON DATA PROCESSORS?

The GDPR, similarly to Directive 95/46/EC, distinguishes between controllers and processors. Controllers determine the "purpose and the means" of the use of personal data, whereas processors process the personal data "on behalf of the controller". Processors can take many forms, from general external service providers, to group companies, software providers, call centres, hosting, IT support, etc. Any external party that has access to personal data and is engaged by the controller is regarded as a "processor".

If the controller wishes to hire a processor, the controller must select one "providing sufficient guarantees to implement appropriate technical and

organisational measures" to ensure the protection of the rights of the data subject and compliance with the GDPR.

Next, the controller must sign a contract with the processor setting out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller, including the appropriate security measures.

The GDPR also gives controllers better insight on the use of subcontractors. The processor cannot outsource the processing to a sub-processor without the written consent of the controller.

## 14 | MY COMPANY PROCESSES PERSONAL DATA ON BEHALF OF OTHER COMPANIES, WHAT DOES THE GDPR MEAN FOR US AS A PROCESSOR?

The GDPR directly imposes greater responsibilities and liabilities on the data processor. The processor has to ensure sufficient guarantees in terms of expert knowledge, its reliability and existence of resources, in

view of implementing the Regulation's technical and organisational measures, and ensure security and confidentiality measures of processing as stipulated by the GDPR. In this respect, controllers and processors that adhere to either an approved code of conduct or an approved certification mechanism may use these instruments to demonstrate compliance with a number of the GDPR's standards.

Processing should be done in compliance with the instructions of the controller and the requirements set by law. The processor should keep records of its processing containing certain elements of information. Should the processor call upon a sub-contracted processor, this party's involvement will need to be agreed upon by the controller. This party will also be subject to the same legal requirements incumbent upon the initial processor.



The processing of data should be governed by a contract (see, Question 14) or other legal act under EU or Member State law, binding the processor to the controller.

This should take into account the specific tasks and responsibilities of the processor in the context of the processing, and the risk to the rights and freedoms of the data subject.

After the processing activities have been done, the processor should either return the data to the controller, or erase it, as per the controller's choice.

Moreover, in the case of any material or immaterial damages arising from violations of the GDPR with respect to data subjects, both controllers and processors can be held liable. A processor will only be exempt from liability if it can prove that it is not in any way responsible for the event giving rise to the damage.

## 15 | DATA BREACH NOTIFICATION: WHAT TO DO WHEN YOUR PERSONAL DATA HAS BEEN BREACHED?

A personal data breach is "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". A breach is thus not limited to a malicious attack on the system. In fact, more often than not, it results from a fault or negligence by the controller's staff (e.g. loss of device). Hence, raising awareness amongst staff through internal policies and trainings is key.

Under the GDPR, controllers in all sectors are required to notify data breaches.

When a controller becomes aware of a data breach, it must notify the competent supervisory authority without undue delay and ultimately within 72 hours (except where reasonably justified). Notification to the supervisory authority is not required when the breach is "unlikely to result in a risk for the rights and freedoms of individuals". When required, the notification must (i) describe the nature of the personal data breach, including the number and categories of data subjects and data records affected; (ii) provide the data protection officer's contact details; (iii) describe the likely consequences of the data protection breach; and (iv) describe how the breach will be addressed, including any mitigation measures taken or proposed.



When the breach is "likely to result in a high risk to the rights and freedoms of natural persons", and subject to limited exceptions, the controller must also communicate information relating to the breach to the data subject without undue delay.

To comply with this obligation, controllers should adopt clear policies for the management of data breaches, which allocate responsibilities and set out the procedures to be followed. This facilitates taking important decisions within the strict timelines imposed by the GDPR in case of a data breach.

## 16 | I WAS INFORMED THAT AS A DIRECTOR OF A COMPANY I HAVE TO APPOINT A DATA PROTECTION OFFICER (DPO). IS THIS TRUE FOR ALL COMPANIES?

The GDPR provides that a controller or processor must designate a data protection officer when: (i) the processing is carried out by a public authority; (ii) it regularly and systematically monitors data subjects on a large scale; or (iii) it processes sensitive personal data on a large scale. In addition Member States can impose additional criteria for appointing a DPO. Companies which do not fall within the aforementioned categories or national criteria, can still appoint a DPO if they so wish. A group of companies may appoint a single DPO if the latter is easily accessible from each establishment within the group.

The GDPR also sets out a profile description of the DPO: he or she must be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices. The DPO may be a staff member or external consultant and may have other (internal or external) tasks in addition to the role of DPO.

The DPO must ensure compliance within the company and therefore may need to defend the interests of data subjects against the (economic) interests of the company. Therefore, the DPO must be independent in the company's organisation, and report to the highest level of management. The DPO is also protected against dismissal or other sanctions for performing his or her tasks.

The data protection officer's tasks include: (i) informing and advising the company on data protection compliance; (ii) advising as regards data protection impact assessments; (iii) monitoring compliance with relevant data protection provisions which includes, for instance, training of staff members and related audits; and (iv) cooperating and acting as a contact point for supervisory authorities.

## 17 | MY GROUP OF COMPANIES OPERATES IN DIFFERENT PARTS OF THE WORLD. CAN I STILL TRANSFER PERSONAL DATA TO COUNTRIES OUTSIDE THE EU/EEA?

To ensure that the protection granted by the GDPR is not undone when personal data is transferred outside of the EU, the GDPR, in principle, only permits personal data to be transferred to third countries which have been found to provide an adequate level of protection by the European Commission (examples include Argentina and New Zealand).

If the recipient of personal data is not established in such a "safe" third country, the transfer will only be permitted if the parties to the transfer provide adequate safeguards. For transfers between private companies, these measures can still take the form of

model contracts adopted by the European Commission or the national supervisory authority, as well as approved Binding Corporate Rules for intra-group transfers. In addition, the GDPR allows safeguards to be adduced by an approved code of conduct or certification mechanism. However, any selected safeguard must ensure that data subjects can enforce their rights and that effective legal remedies are available to the data subjects in relation to the transfer.

Finally, for transfers which are not massive, repeated or structural, the GDPR provides derogations, such as requesting consent, or transferring data that is necessary for the defence of legal claims.

### 18 | TO WHICH SUPERVISORY AUTHORITY SHOULD I REPORT?

The GDPR creates a new EU data protection authority, the EDPS, to ensure the consistent application of the GDPR throughout the EU. The EDPS provides guidance and mediates between national supervisory authorities when needed.

The supervisory authorities remain competent for the enforcement of the GDPR within their Member States. For multinational groups having various establishments throughout the EU, the main establishment will determine the Lead Supervisory Authority (**LSA**) which will act as a one-stop-shop for the group's data protection enforcement. The one-stop-shop mechanism does not apply to companies that are not established within the EU (even if the company has a local representative in the EU).

Notwithstanding the one-stop-shop, data subjects can file complaints with the supervisory authority of their habitual residence, place of work or place of the alleged

infringement, even in those situations where the activities are carried out by non-EU data controllers or processors.

In situations of cross-border processing of personal data which substantially affects data subjects in more than one Member State, one authority will take the lead and coordinate between the other supervisory authorities concerned. The LSA is required to liaise and cooperate with other concerned supervisory authorities on the basis of mutual assistance. Joint operations have been put in place, for instance, to monitor the implementation of a measure concerning a controller or processor established in another Member State.

In specific cases, the EDPS must issue an opinion to a supervisory authority, or act as a dispute resolution body by adopting binding decisions, for instance when a supervisory authority expresses an objection to a draft decision of the LSA.

### 19 | DOES THE REGULATION PROVIDE FULL HARMONISATION OR ARE THERE DIFFERENCES BETWEEN MEMBER STATES?

Although the GDPR is a Regulation which is directly applicable in all Member States as from 25 May 2018, there is still room for some national variations, since the Regulation provides for derogations to national provisions in over 60 instances. Examples of possible disparities between Member States are the age for children's consent (which may vary between 13 and 16 years old), the criteria for appointing a DPO, as well as the specific rules that Member States may provide in relation to the processing of employees' personal data in an employment context and the processing of personal data for archiving or scientific purposes. Member States can also provide for exceptions to the right of data subjects, or impose specific conditions for processing sensitive personal data or data relating to criminal convictions and offences.

Moreover, national supervisory authorities are the primary enforcers of the data protection rules, which will inevitably result in differences over how data protection rights are enforced between Member States.

Other differences between Member States may also arise from Directive 2016/680 on the processing of personal data by the police and the criminal justice sector. The directive is not directly applicable. This means that, when transposing the directive into their legislation, Member States each determine the most appropriate means to achieve the goals laid down in the directive.

### 20 | HOW DO I ENSURE THAT MY ORGANISATION IS GDPR COMPLIANT?

Setting up an adequate structure and determining responsibilities is an essential first step. Raising data protection awareness and implementing appropriate policies and procedures at an early stage facilitates compliance in the long run.

On the operational level, compliance begins with assessing your current situation in order to be familiar with your data processing activities. Existing processing operations must be registered. Based on these findings, which may require conducting a data protection audit, you need to assess the impact of the GDPR on your data processing activities and identify the gaps.

Next, you need to set your priorities in addressing the gaps, taking into account the relevant risks.

Data protection compliance is an ongoing exercise. This means that new data processing activities need to be assessed before they are implemented and that policies, procedures and security measures have to be monitored and regularly reviewed, and also the changes in processing of personal data have to be captured and documented, with, amongst other things, staff awareness being raised and maintained.

### 21 | WHAT IS THE RISK IF MY ORGANISATION FAILS TO COMPLY WITH DATA PROTECTION RULES?

The GDPR provides the supervisory authorities with an array of corrective powers, such as warnings or reprimands; temporary processing bans; suspension of international data flows; orders to grant access to data subjects, correct or delete personal data; and finally administrative fines.

Supervisory authorities determine the most appropriate corrective action(s) for each specific situation. Reprimands are mainly chosen for "minor" infringements. Conversely, administrative fines are imposed where the infringement poses a significant risk to the rights of the data subjects concerned. For example, this will be the case when processing gives rise to discrimination, identity theft or fraud, damage to reputation or when sensitive categories of personal data or personal data of vulnerable persons are processed.

Fines will also be preferred when processing involves a large amount of personal data and affects a large number of data subjects or if an infringement has not been remedied in a timely manner. Fines can go up to EUR 20 million or 4% of the company's total annual worldwide turnover (whichever is higher).

Aside from complaining to supervisory authorities, data subjects suffering material or non-material damages as a result of a GDPR infringement may claim compensation in court proceedings.

The GDPR entitles representative non-profit organisations acting on behalf of data subjects to lodge complaints with supervisory authorities and seek judicial remedies against data controllers or processors.

Glaverbel Building  
Chaussée de La Hulpe 166  
Terhulpesteenweg  
B-1170 Brussels  
Belgium

Phone: +32 (0)2 647 73 50

Fax: +32 (0)2 640 64 99

[vbb@vbb.com](mailto:vbb@vbb.com)

[www.vbb.com](http://www.vbb.com)