GDPR Q&A | Twenty Questions and Answers to assist companies in preparing for 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, Directive 95/46/EC further elaborates on the rights and obligations when processing personal data. Notably, in the Spring of 2018, a new "General Data Protection Regulation" (***GDPR***) will enter into force, replacing the current and outdated framework of Directive 95/46/EC and its national implementing laws.

The new GDPR contains significant new obligations, when compared to the old regime 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. 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 data protection authorities (***DPAs***) 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 preparing for the implementation of 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.

Chaussée de La Hulpe 166 Terhulpsesteenweg
B-1170 Brussels – Belgium

Phone: +32 (0)2 647 73 50
Fax: +32 (0)2 640 64 99

vbb@vbb.com
www.vbb.com

VAN BAEL & BELLIS

GDPR Q&A | Twenty Questions and Answers to assist companies in preparing for the General Data Protection Regulation

| CONTENTS

Chaussée de La Hulpe 166 Terhulpsesteenweg
B-1170 Brussels – Belgium

Phone: +32 (0)2 647 73 50
Fax: +32 (0)2 640 64 99

vbb@vbb.com
www.vbb.com

1 | WHEN WILL THE NEW GDPR ENTER INTO FORCE AND WILL THE REGULATION PROVIDE FULL HARMONISATION OR WILL THERE BE DIFFERENCES BETWEEN MEMBER STATES?

At the time of writing, the GDPR still needs to be formally adopted by the European Parliament and the Council. However, this formal adoption and publication in the Official Journal is expected in the spring of 2016. The GDPR will be directly applicable in each Member State two years and twenty days from its date of publication in the Official Journal.

This transition period is much needed as it will allow companies to plan for compliance with the GDPR and Member States to bring their national laws in line with the new Regulation. During this time, the European Commission, the DPAs and the newly created European Data Protection Board (***EDPB***) (see, Question 19) will issue guidance on the application of the GDPR.

Although the GDPR is a Regulation which is directly applicable in all Member States, there is still room for some national variations, since the Regulation provides for derogations to national provisions in over 60 instances. Moreover, national DPAs will be the primary enforcers of the data protection rules, which will inevitably result in differences over how data protection rights are enforced between Member States.

2 | 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 will still likely be 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 company. Moreover, if these personal data are being handled by third parties, such as a 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 will be affected by the GDPR.

3 | I HEARD THAT WE WILL NO LONGER NEED TO FILE A NOTIFICATION FOR EACH PROCESSING. IS THAT TRUE?

Under Directive 95/46/EC, most Member States' laws require that automated processing of personal data is notified to the local data protection authority. For many companies, the notification or registration with the national DPA was a key element of their data protection compliance program.

The obligation to notify data processing activities will no longer exist under the GDPR. In general, there are fewer contacts with data protection authorities under the GDPR (except, among others, data breach notifications or negative data protection impact assessments). The European Commission considered that the notification obligation

had resulted in a formalistic approach towards data protection compliance. Instead of notifying to the public authorities, the GDPR will oblige companies to maintain up-to-date internal records on their processing of personal data, containing similar information to the current notifications. Hence, existing notification documents can provide a useful starting point for these internal records. Needless to say, the obligation to keep up-to-date internal records will place a significant burden on controllers. However, and subject to certain conditions, SMEs will be 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.

4 | 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 DPAs and to data subjects that it is treating personal data in compliance with the GDPR.

By specifically referring to *accountability,* the GDPR is likely to shift the manner in which organisations and DPAs approach data protection compliance, encouraging data controllers to do so in a more pro-active (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 3); (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 8); (vii) and appointing a Data Protection Officer (see, Question 17). Depending on the situation, these actions are obligatory under the GDPR.

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

5 | 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.

6 | 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 will be 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.

7 | WILL IT STILL BE POSSIBLE TO RELY ON IMPLICIT CONSENT?

Consent remains a lawful basis to transfer personal data under the GDPR. However, the definition of consent is significantly restricted. While Directive 95/46/EC has allowed controllers to sometimes rely on implicit and 'opt-out' consent (as long as it was "unambiguous"), the GDPR will now require 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 has been based on consent, it is not necessary for the data subject to give their consent again if the way in which the consent was given is in line with the conditions of the GDPR.

While under Directive 95/46/EC consent could be inferred from an action or inaction, by requiring the data subject to make a statement or a clear affirmative action to express consent, the GDPR eliminates the possibility of implicit or 'opt-out' consent.

Furthermore, consent must be specific to each data processing operation, and "clearly distinguishable" from any other matters in a written document. The GDPR also allows data subjects to withdraw consent at any time, making it "as easy to withdraw consent as to give it". Controllers must inform the data subjects of their right to withdraw consent before consent is actually given. 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.

There are some more specific cases of 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 | WILL 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 4), 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 DPAs, whereas seals or certifications will be granted by certification bodies, DPAs or the EDPB.

DPAs shall encourage the development of codes to take account of the specific features of particular industries and sectors. Where a DPA 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.

9 | 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 will have to review their contact points, such as the various interfaces where a company provides information to data subjects, to ensure that any notice complies with the new 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 DPA and the contact details of the 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 subjects 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 will be 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.

10 | WILL 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 subjects have the right to object to the use of profiling (depending on the legal basis of the processing and possible overriding interest of the controller). Automated profiling which significantly affects the data subject can, in most cases, only be possible when it is necessary for the performance of a contract, a legal obligation, or with the explicit consent of the data subject.

The GDPR also prohibits profiling decisions based on sensitive personal data, and systemic use of profiling will require a prior data protection impact assessment.

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

The GDPR, as well as the current 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 comply 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.

12 | 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 their processing containing certain elements of information. Should the processor call upon a sub-contracted processor, this party's involvement will need to be agreed

to 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 11) 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.

13 | 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 exempt 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.

The GDPR directly imposes greater responsibilities and liabilities on the data processor.

14 | 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, but can also result from a fault or negligence by the controller's staff. 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 DPA without undue delay and ultimately within 72 hours (except where reasonably justified). Notification to the DPA 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 risk for the rights and freedoms of individuals", and subject to limited exceptions, the controller must also communicate information relating to the breach to the data subject without undue delay.

Controllers should prepare for this obligation by adopting 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.

15 | HOW CAN THE DATA SUBJECT 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.

Preparing for the GDPR and complying with its obligations once it enters into force will require a significant commitment from companies.

This right builds upon the right to be forgotten identified by the European Court of Justice in *the Google Spain v AEPD and Mario Costeja Gonzales* case in 2014. The Court in that case required search engines to remove links to webpages that appear when searching a person's name, at that person's request. The search engine could only refuse to comply with this request if it was in the "preponderant interest of the general public" to have access to the information in question.

The GDPR codifies this right, which will apply 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, or the processing was unlawful.

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

16 | 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 a contract, and does not apply to processing based on a public interest or the controller's legitimate interests.

17 | 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) processes sensitive personal data on a large scale. A group of companies may appoint a single data protection officer 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 member and related audits; (iv) and cooperating and acting as a contact point for DPAs.

18 | MY GROUP OF COMPANIES OPERATES IN DIFFERENT PARTS OF THE WORLD. CAN IT 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, 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.

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 DPAs, 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.

19 | DOES THE GDPR SET UP A CENTRAL EU DATA PROTECTION AUTHORITY?

The GDPR creates a new EU data protection authority, the EDPB, to ensure the consistent application of the GDPR throughout the EU. The EDPB will provide guidance and mediate between national DPAs if needed. The DPAs remain competent for the enforcement of the GDPR within their Member States.

The DPA of the main establishment of a multinational group of companies will determine the lead authority which will act as a one-stop-shop for the group's data protection enforcement. However, there are some significant limitations to the one-stop-shop principle. The lead authority will cooperate with other concerned 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 EDPB must issue an opinion to a DPA, or act as a dispute resolution body by adopting binding decisions, for instance when a DPA expresses an objection to a draft decision of the lead authority.

20 | THE GDPR LAYS OUT SUBSTANTIALLY MORE PROVISIONS THAN DIRECTIVE 95/46/EC. THEREFORE, WHERE DO I START?

Preparing for the GDPR and complying with its obligations once it enters into force will require a significant commitment from companies. Setting up an adequate structure and determining responsibilities will be an essential first step. Raising data protection awareness and implementing appropriate policies and procedures at an early stage will facilitate compliance in the long run.

On the operational level, preparation begins with assessing your current situation in order to become familiar with your data processing activities. Based on these findings, which may require conducting a data protection audit, you will need to assess the impact of the GDPR – for each obligation – on your data processing activities and identify the gaps. Next, you will 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 policies, procedures and security measures will have to be monitored and regularly reviewed, and also the changes in processing of personal data will have to be captured and documented, with, amongst other things, staff awareness being raised and maintained.

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

Phone: +32 (0)2 647 73 50
Fax: +32 (0)2 640 64 99

vbb@vbb.com
www.vbb.com