AWDC | *Q&A on GDPR for the Diamond Sector*

Version of 22 June 2018

TABLE OF CONTENTS

1. WHEN DO I, AS A DIAMOND TRADER, NEED TO APPLY THE GDPR?

The GDPR (General Data Protection Regulation) applies to anybody who is processing personal data. Personal data is any information that relates to a human being, whether you know that person ("identified") or whether you may be able to identify that person by using an identification number, cookies or any other specific characteristics or details of that person ("identifiable").

In other words, the definition of "personal data" is very wide and covers almost any information that can be connected to an individual. Accordingly, as a diamond trader, you will need to apply the GDPR in case you process personal data of your employees, your customers, your suppliers or anyone else. Therefore, you must keep in mind that, even when you do not use their personal data to specifically target customers (for example, by sending advertisements), the GDPR will still likely be applicable to you since you collect personal data during your professional activities.

2. WHEN DO I NEED TO START ACTING IN COMPLIANCE?

From **25 May 2018** onwards, the GDPR will become applicable to all companies based in the European Union, including to diamond traders. Even if you are not based in an EU country, but you offer products or services to people living in the European Union, you will have to comply with the GDPR rules.

3. AM I A DATA CONTROLLER OR A DATA PROCESSOR?

The GDPR distinguishes between "data controllers" and "data processors". Each have different responsibilities:

- **"Controllers"** determine the **"purpose and the means"** of the processing of personal data. In other words, if you decide yourself what kind of personal data you process, for which purposes you process these data, and which technology you use to process the data, then you will be a data controller. In general, as a diamond trader, you will be considered to be a data controller. Furthermore, as a diamond trader, you normally hire several processors, such as IT services providers, security services providers, etc.

- **"Processors"** process the personal data **"on behalf of the controller"**. Accordingly, if you merely act on instructions of another company, and you do not decide yourself which data is to be processed or for which purposes, then you are a processor. Processors can take many forms e.g. external service providers, hosting providers, IT support providers, etc.

4. HOW DO I MAKE SURE THAT I ACT IN COMPLIANCE WITH GDPR AND DEMONSTRATE IT?

The data controller is responsible for and must be able to demonstrate compliance with the requirements under the GDPR (the **"accountability principle"**). This requires you to implement a compliance strategy that is able to monitor compliance throughout your organization and demonstrate to the Data Protection Authority (DPA) and to data subjects that you are processing personal data in compliance with the GDPR. In the following answers it will become clear what you can do to comply with this accountability principle. A good way to start is to obtain a certificate of attendance of an AWDC café GDPR and/or any other data protection seminars you may have attended. Furthermore, future AWDC AML & Compliance seminars will include the topic "GDPR", which means that you can use your certificate of attendance to demonstrate that you undertake efforts to inform yourself on and to act in compliance with the GDPR.

5. WHO WILL CONTROL WHETHER OR NOT I COMPLY WITH GDPR?

In Belgium, you will be controlled by the Data Protection Authority (www.privacycommission.be). The Data Protection Authority enjoys wide investigative and corrective powers including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities. They will also have the competence to issue sanctions. Also third parties can file a complaint with the Data Protection Authority or initiate a claim against you if you are storing their data in an unlawful manner.

6. DO I NEED A LEGAL BASIS FOR PROCESSING PERSONAL DATA?

Diamond traders typically process personal data of their employees, their customers, their suppliers or other persons they are in contact with. Personal data could be contact details of your clients and suppliers, social security numbers of your personnel, the KYC information of your customer such as an identity card / passport information, camera surveillance footage, fingerprints assembled for security reasons, or any other information relating to a human being.

Before continuing to read this Q&A, it is useful if you map out all the personal data that you process in order to have a clear overview of the data and data flows. After doing this, you have to make sure that the personal data is processed based on at least one of the six lawful bases mentioned in Article 6 (1) of the GDPR. In particular with regard to you as a diamond trader, the following four **lawful bases are relevant**:

- **Consent** – orally or in writing. It is important to note that consent is one lawful basis for processing. There are alternative legal bases which may be more preferable because consent can in some circumstances be difficult to obtain. Therefore, you should only ask for consent in case you cannot rely on any other legal basis (see below).

  The GDPR has significantly restricted the definition of "consent". As a result, the GDPR requires

the data subject to show agreement by a statement or a "clear affirmative action", like ticking a box or swiping the screen. In addition, consent must be "freely given, specific and informed" and diamond traders will need to be able to demonstrate that consent was given. Consent is appropriate if you can offer people a real choice and control over how you use their data, and want to build their trust and engagement. If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis, because it may not be considered to be freely given.

For example, consent will be relevant when you undertake **direct marketing** activities (promoting products/services to clients/potential clients via e-mail or other). See question 9 for more information on direct marketing.

Explicit consent is only required in certain specific circumstances such as the processing of sensitive data (see below, question 11). Explicit consent must be expressly confirmed in words, rather than by any other positive action such as clicking or ticking a tick box (e.g. by means of a signed written statement). For example, fingerprints are considered to be sensitive data and thus explicit consent should be obtained to process this type of data.

Note: where other grounds apply, e.g. a legal obligation such as anti-money laundering legislation, for the processing of sensitive data, you will not need to ask the data subject his/her explicit consent.

- **Performance of a contract** – you can rely on this lawful basis if you need to process someone's personal data (i) to fulfil your contractual obligations towards them (e.g. you need data of your employee in order to pay his salary or execute the employment agreement); or (ii) because they have asked you to do something before entering into a contract (e.g. provide a quote). With a view to acting in accordance with the accountability principle, you should document your decision to rely on this lawful basis and ensure that you can justify your reasoning.

  For example, your HR department needs to request and process personal data of staff in order to be able to fulfil the employer's obligations under the **employment contract**, such as the payment of the salary (see question 8 for a more detailed explanation on your GDPR obligations towards employees). You may also process **personal data of clients or suppliers** because you have a contractual relation with them and you need their data for invoicing and shipping (e.g. their contact details and address).

- **Legal obligation** – sometimes you can rely on a legal obligation, meaning that a law allows you to store personal data.

  For example, anti-money laundering legislation (AML) allows you to process KYC data of your client, and personal data related to criminal convictions (see question 10 below on the correlation between the AML and the GDPR) or your social security obligations regarding your employees require you to process your employees' personal data;

- **Legitimate interests** – this is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate. Relying on this lawful basis implies that you can demonstrate that you have a valid interest in processing certain personal data. However, this lawful basis will not apply if your legitimate interests are overridden by the interests or fundamental rights and

freedoms of the data subject.

For example, diamond traders are not required to ask data subjects their consent when using **surveillance cameras (CCTV)** because it is your legitimate interest to have such cameras for security purposes. Keep in mind that you still need to comply with the obligations under the (new) Law on Cameras as well as the requirements under the GDPR that are not regulated in the Law on Cameras. Moreover, in case you are using CCTV you should carry out a **data protection impact assessment (DPIA)** because CCTV is considered to be a processing activity that is likely to result in a high risk to the rights and freedoms of individuals. A DPIA helps you identify and minimize the data protection risks of high risk data processing activities. As regards CCTV, the assessment will be an easy task if you can demonstrate compliance with the (new) Law on Cameras. The assessment can take the form of a questionnaire which you need to complete and based on the answers provided, you will be better able to assess whether further actions should be undertaken to comply with your obligations under the GDPR (an example of such questionnaire can be found here.

It can be concluded that you don't always have to rely on consent as the lawful basis for processing of personal data. We advise you to always assess whether there is a more appropriate legal basis than consent. It is also important to assess which legal basis applies to each personal data processing activity that you undertake, since you are required to inform the data subject about the legal basis of the processing (see question 7).

7. WHAT INFORMATION DO I NEED TO PROVIDE TO THE DATA SUBJECT?

Once you have defined the correct lawful basis for the personal data you process, you have to inform the data subject on the fact that you are processing his/her data. As personal data must be processed lawfully, fairly and in a transparent manner (the **"lawfulness, fairness and transparency principle"**), you must inform any data subject in advance how and for which purpose you will collect his data and that such processing is based on a lawful basis such as consent, a contract, a legal obligation or a legitimate interest.

You can inform data subjects such as (future) customers and suppliers by means of a privacy statement on your website and/or by providing them with a physical copy of a privacy statement before you start processing their personal data (a template of such privacy statement can be found here. If you don't have a website, you can for example provide the client with a copy of your privacy statement at the reception. You could also include a reference to your privacy statement on your invoice or attach a copy of such privacy statement to the invoice. It is not required to proactively inform data subjects about your new privacy statement. In other words, it is not necessary to send emails to your existing clients about your new privacy policy.

You also have to inform your employees in their capacity as data subjects via a separate employee privacy notice (a template of an employee privacy statement can be found here).

The AML also requires you to provide your clients with a general notice regarding your obligation under the AML to process certain personal data in the context of preventing money laundering and

terrorism (a template of such a notice can be included in your e-mails or your client letters when asking for KYC-information, or even on your invoice. A Template of such a notice can be found here);

Where you obtain personal data from a data subject you must provide the data subject with information about the processing, notably the following information which can also be found in the templates of the privacy statements that AWDC drafted for the diamond sector (as mentioned higher):

- the identity and contact details of the controller;
- where applicable, the contact details of the data protection officer;
- the purposes of processing and the lawful basis for the processing;
- the (categories of) recipients of the data;
- information on applicable safeguards in the context of a transfer outside of the EEA;
- information on the existence of the data subject rights (right to access, rectification, erasure ["right to be forgotten"], right to withdraw consent, etc.);
- the nature of the requirement to provide the data (contractual or legal requirement) and the possible consequences of failure to provide such data;
- storage period;
- the right to lodge a complaint with a supervisory authority; and
- if applicable, the existence of automated decision-making, including profiling and meaningful information about the logic involved.

8. WHAT ARE THE CONSEQUENCES OF THE GDPR IN AN EMPLOYMENT CONTEXT?

You will most likely employ a few employees in your company and therefore process "employee data" (i.e. personal data that you receive from your employees within the context of the employment of that employee). Accordingly, many aspects of the GDPR will apply to you, such as:

- As regards the legal basis, you will in most cases be able to rely on the performance of a contract, notably the employment contract or on the legal obligation, for example with regard to social security obligations.
- You should avoid to rely on consent with regard to employee data, since consent under the GDPR is subject to strict requirements and must be freely given as well as specific, informed and unambiguous. It is deemed that consent obtained in an employment context is most likely not

freely given due to the imbalance of power between the employer and the employee.

- You need to inform your employees on the processing of their personal data, for example through an employee privacy notice (see question 7 - a template of an employee privacy statement can be found here.
- Your employees can exercise their rights (see question 22) such as the right to receive a copy of the personal data which you hold about them.
- To demonstrate that your company is taking measures to comply with the GDPR, it is recommended to provide your employees with instructions on how they should handle personal data and to organize data protection trainings from time to time. Your employees could participate in the compliance seminars of AWDC where the GDPR topic is covered.
- Also ensure security and confidentiality by all your employees involved in the processing of personal data, e.g. by including or amending the confidentiality clause in the employment contract in order to also protect personal data - an example of such clause can be found here.

9. CAN I SEND DIRECT MARKETING COMMUNICATIONS TO MY CUSTOMERS?

Direct marketing, such as newsletters and other email communications in order to inform customers about a product or service, is not only regulated by the GDPR but also by other sets of rules, such as the ePrivacy Directive. Accordingly, you can only send marketing texts and emails to individuals if that person has specifically consented to receiving them. Furthermore, you must provide the individual with a possibility to opt out or unsubscribe (i.e. withdraw consent).

However, with respect to existing customers, you can send marketing texts or emails without requesting consent if the following three conditions are met:

- You have obtained the contact details of the individual in the course of a sale of a product or service to that individual;
- The marketing texts or emails are only marketing your own similar products/services (and thus not products/services of other companies or your own products/services which are different from the products/services you have promoted to the existing customer in the past); and
- You gave that individual the opportunity to refuse or opt out of the marketing, both when first collecting the details and in every message after that.

In other words, if these conditions are met, you can send such marketing communications to your existing clients. Keep in mind, however, that you cannot send such communications to a client that opted out of such direct marketing communications (e.g., when the client did not tick the tick-box providing him the possibility to receive such direct marketing communications, or when the client unsubscribed from the mailing list). “Existing customers” relates to the persons with whom you entered into a client relationship with.

This means that with respect to new potential customers with whom you have not (yet) established a client relationship, you will need to ask them for consent before sending direct marketing communications, e.g. by including a tick box where the interested party can confirm or refuse that he/she wants to receive newsletters and that his/her data can be processed for that purpose. Keep in mind that consent should be freely given. This implies that you cannot "bundle" consent with acceptance of terms and condition, or "tie" the provision of a contract or a service to a request for consent to process personal data that are not necessary for the performance of the contract or the service (e.g. promising a gift upon giving consent to subscribe to your newsletters, or denying services in case of refusal). We therefore recommend developing a consent form which can be used and sent by e-mail to ask data subjects for consent, where applicable. You can find an example of such consent form here:

In addition, don't forget you must inform data subjects, for example, by means of a privacy statement on your website or by providing (future) customers or suppliers with a physical copy of a privacy statement before you start processing their personal data (a template of such privacy statement can be found here.

10. WHAT IS THE CORRELATION BETWEEN THE GDPR AND AML?

Both the GDPR and AML will influence each other, in particular with regard to the following points:

- AML can serve as a lawful basis to process particular personal data, as it imposes a legal obligation on diamond traders to collect and store certain personal data (e.g. identity information);
- but the personal data processed in the context of compliance with a legal obligation cannot be used for any other purpose (e.g. marketing purposes). Furthermore, even if you would ask consent to use UBO data for marketing purposes, this is not allowed, since UBO data relates to data of third parties for which your client cannot give consent;
- the fact that your lawful basis is a legal obligation does not exempt you from your information obligation towards the data subjects (see question 7 above). We also recommend including the general notification, which is required under the AML, in all your communications such as letters or emails, you can find it here. You should also inform data subjects about the possibility that their data can be transferred to third parties, e.g. to financial institutions or public authorities;
- the GDPR does not prejudice the obligation under the AML to keep certain data for 10 years. However, after those 10 years, the data which is to be processed for AML purposes, have to be deleted (see question 16 below);
- the rights of data subjects regarding their personal data are limited under the framework of the AML (see question 22 below);
- other parties that are subject to the AML (e.g. financial institutions) can rely on their obligations under the AML as well to request certain information from you (e.g. identity information of your customers or suppliers);

- within the framework of your obligations under the AML, you are allowed to process personal data related to criminal convictions and offences.

11. ARE SOME DATA MORE SENSITIVE THAN OTHERS?

Processing sensitive data is, in principle, prohibited by the GDPR, unless one of the exceptions applies. Sensitive data is defined in the GDPR as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of generic 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.

As a diamond trader, you would generally not come into contact with sensitive data. However, if a fingerprint system is used for security reasons, that would qualify as sensitive data. In that case, you will need to request "explicit consent" from the data subject (see question 6 above).

12. CAN I PROCESS PERSONAL DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES?

The AML legislation allows diamond traders to process personal data relating to criminal convictions and offences, but only for the purpose of compliance with your obligations under the AML. The AML will thus also serve as your lawful basis in accordance with Article 6(1) GDPR to be allowed to process such personal data.

Therefore, you are also authorized on the basis of your KYC obligations under the AML to consult, for example, the Bureau Van Dijk database which contains personal data relating to criminal convictions (such as UN sanction lists).

Keep in mind that you can only process such data for the purposes of complying with your obligations under the AML.

13. CAN I USE THE DATA FOR WHATEVER PURPOSE?

You cannot use personal data that is processed for a certain purpose for other incompatible processing activities (the **"purpose limitation principle"**).

For example, personal data that you have collected for anti-money laundering purposes cannot be re-used for direct marketing purposes without asking the data subject for consent. The same applies if you have collected Ultimate Beneficial Ownership (UBO) information from your client. You cannot use this information to approach its UBOs to try to sell diamonds to them.

14. CAN I COLLECT AS MUCH DATA AS I WANT?

You can only collect adequate, relevant data, which is limited to what is necessary in relation to the purpose(s) for which you collect the data (the **"data minimization principle"**). This means you cannot collect more data than you need in accordance with the purposes for which you collect the personal data.

For example, the AML legislation requires you to identify your clients, but this does not allow you to collect more information than what is necessary (e.g. it is not allowed to request your client's license plate number).

15. WHAT DO I NEED TO DO TO PROTECT THE PERSONAL DATA WHICH I PROCESS?

Data must be processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the **"integrity and confidentiality principle"**).

You can, for example, make sure that only certain authorized staff has access to the personal data and that access to such data is logged (meaning that an audit trail is kept of who accesses the personal data and when).

We also recommend implementing internal policies and compliance procedures (e.g. a privacy policy for internal purposes, notably to instruct your employees how they should handle, store, disclose and otherwise process personal data). You can find an example of an internal privacy policy, that we made specifically with respect to the diamond sector here.

Also ensure security and confidentiality by all internal and external parties involved in the processing of personal data, e.g. through the execution of a non-disclosure agreement with third parties that access personal data in your company or through confidentiality obligations in an employment contract (by including or amending the confidentiality clause in the employment contract in order to also protect personal data - an example of such clause can be found here.

16. CAN I KEEP THE DATA AS LONG AS I WANT?

According to the GDPR, personal data should not be kept for longer than is necessary for the purposes for which the personal data are processed (the **"storage limitation principle"**). You should put in place technical and organizational measures in order to make sure that personal data is deleted or returned in due time. For example, make a record of retention periods for different types of personal data or install an automated process for the deletion of personal data when the retention period has elapsed.

As a diamond trader, you are obliged by the AML to store identification data for 10 years as from the end of the business relationship or as from the date of an occasional transaction (see, Article 60 (1)

1° AML). This means that you should make sure that the personal data is deleted or returned when the period of 10 years is expired. Furthermore, you should also keep your invoices for 10 years, i.e. the statute of limitation for civil liability. Any other personal data should thus not be stored for longer than is necessary and therefore you should put in place specific retention periods.

17. DO I NEED TO KEEP THE DATA UP-TO-DATE?

Data processors need to make sure that the data which they process are accurate and, where necessary, kept up-to-date (the **"accuracy principle"**). This means that, for your internal organization, you should keep track of your processing activities and put in place technical and/or organizational measures to comply with the obligation to keep information accurate and up-to-date.

For example, you can designate a person in your company who is responsible for verifying annually whether the information collected is still accurate and up-to-date or implement self-service tools that the data subject can use to keep its information up-to-date.

18. DO I NEED TO DOCUMENT MY PROCESSING ACTIVITIES?

In principle, only companies with more than 250 employees are required to maintain a formal record of their processing activities. This means keeping detailed and up-to-date documentation on the processing of personal data that you update if you engage in new processing activities such as sending newsletters to clients which you did not do before.

However, companies with less than 250 employees will also need to maintain such record if:

- it is likely that the processing of the personal data results in a risk to the rights and freedoms of the data subjects; or
- the processing is not occasional; or
- the processing includes sensitive data or data relating to criminal convictions or offences.

Processing that is occasional should be understood as processing that is coincidental, unforeseen or unusual. Since diamond traders are required under the AML to process identification data before engaging a new client, such processing will likely be considered too systematic to be merely "occasional", thus you will need to establish such register. Furthermore, it is also possible that you are processing data relating to criminal convictions (such as the UN Sanction List that is available in the Bureau Van Dijk database) which also results in the obligation to establish such register.

The GDPR determines which information should be included in such a record:

- the name and contact details of the controller (that is the diamond trader);
- the purposes of the processing (e.g. compliance with KYC obligations under the AML);

- a description of the categories of data subjects and of the categories of personal data (e.g. customers and their identification data);
- the categories of recipients with whom personal data is shared (e.g. financial institutions);
- where applicable, transfers of personal data outside the European Economic Area (EEA);
- where possible, the retention periods of the different categories of data (e.g. the limitation period of 10 years under the AML for identification data); and
- a general description of the security measures (e.g. only authorized staff has access to the data or encryption of the data).

Below you can find an example of a record of processing activities which you can use for your company:

Data controller: [INCLUDE DETAILS OF DATA CONTROLLER: name & legal form, registered office]						
Categories of data subjects	Purposes	Categories of personal data	Categories of recipients of the personal data	Retention period (when will the data be deleted?)	Transfers of personal data to third countries (incl. documentation of suitable safeguards where applicable)	Technical and organization security measures
Employees	Employee management (e.g. pay-roll, social security, etc.)	Identification data (such as name, address, telephone, etc.); financial data (such as bank account details)	Social security institutions, pay-roll service providers, etc.	Contractual documentation will be retained until 7 years after termination of the employment contract in accordance with statutory provisions on social fraud.	No	E.g. logging and access control, encryption, password and log-in, etc.

19. CAN I SHARE PERSONAL DATA WITH THIRD PARTIES?

As a diamond trader, it is possible that you are required to share personal data with third parties, such as IT service providers, affiliated companies, financial institutions and authorities (for example, within the framework of the AML or the Responsible Jewelry Council). In case you share the personal data which you process with third parties, you need to have a legal basis to do so, as always, and you need to do this in a transparent manner and inform the data subjects about the fact that their personal data can be shared and the possible recipients of the data. This information is included in the privacy statement, thus it is not necessary to inform data subjects separately thereof.

Furthermore, to ensure that the protection granted by the GDPR is not undermined when personal data is transferred outside the EU, the GDPR, in principle, only permits transfers of personal data to third countries which have been found to provide an adequate level of protection by the European Commission. In that case, transfers to such third countries will be assimilated to personal data transmissions within the European Economic Area (EEA).

The list of third countries that provide an adequate level of protection can be accessed here. So far, the European Commission recognized Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US as providing adequate protection.

As regards the US, transfers of personal data will occur within the framework of the so-called "EU-US Privacy Shield". This framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the US for commercial purposes.

As far as other third countries, other than those mentioned above, are concerned, appropriate safeguards should be taken to guarantee an adequate level of protection of the personal data in question. With respect to affiliated companies, a data transfer agreement could be concluded between the transferring party and the receiving party. This document stipulates the rights and duties of the transferring party and the receiving party as well as how the personal data is protected both during and after the transfer. The European Commission has made templates of such agreements, which can be accessed here (for EU data controller to non-EU data controller situations) and here (for EU data controller to non-EU data processor situations).

For groups which have many companies situated in different geographical regions, an intra-group data transfer agreement (IGDTA) could be concluded. This is one lengthy document to be agreed upon and signed by all affiliated companies and thus follows a more rigid procedure. For practical reasons, it is recommended to use the data transfer agreement templates by the European Commission in all bilateral relations between which data is transferred between the EU and non-EU countries which are not on the European Commission list, when there is a limited number of parties between whom data is shared.

The GDPR also recognizes the following measures as appropriate safeguards for the transfer of EU personal data to a third country:

- Binding corporate rules;
- Standard contractual clauses adopted by the European Commission;
- An approved code of conduct; or
- An approved certification mechanism.

For example, when your company shares KYC information with an associated company in a third country that is not recognized as providing adequate protection, you will need to make sure that firstly, you have a legal basis to do so (this may be in your legitimate interest) and secondly, that you take appropriate measures to guarantee an adequate level of protection (by concluding a data transfer agreement or intra group transfer agreement for all personal data which may be shared within the group). However, also bear in mind that when you share particular data, such as KYC, with your affiliated companies, they need to have a legal basis to process this information as well. For KYC data, this means that they need to be subject to a legal framework which requires them to identify their clients as well. If your affiliated company has no legal basis whatsoever to collect KYC information, you cannot share your KYC data with them.

20. CAN I OUTSOURCE SOME OF MY DATA PROCESSING ACTIVITIES?

As a diamond trader, it is possible that you outsource some of your data processing activities, such as to IT services and security services. In those cases, you must work with service providers who are "providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject".

Furthermore, you will need to sign a contract with each processor you hire. That contract must contain at least the following:

- subject-matter of the processing;
- duration;
- the nature and the purpose of the processing;
- the type of personal data and categories of data subjects;
- the obligations and rights of the controller.

In addition, the contract must stipulate specific clauses that describe certain obligations of the processor (e.g. follow the documented instructions from the controller; take appropriate technical and organizational measures, do not engage a sub-processor without prior written consent of the controller, etc.).

Note that most processors that you work with probably already have such clauses in the contracts that you have signed with them. For example, Microsoft's amendment to its online subscription agreement includes a data processing agreement, which can be accessed here. Of course, it cannot hurt to double check with your data processors if such clauses are in place.

21. DO I NEED TO APPOINT A DATA PROTECTION OFFICER (DPO)?

A Data Protection Officer (DPO) needs to be appointed if one of the following situations applies:

- processing is carried out by a public authority;
- regularly and systematically monitoring of data subjects on a large scale; or
- processing of sensitive data on a large scale.

A DPO cannot be dismissed or penalized for performing his/her tasks. In this regard, DPOs enjoy a certain degree of employment protection. Furthermore, a DPO is bound by secrecy or confidentiality concerning the performance of his/her tasks.

Based on the above, it is not likely that you, as a diamond trader, will need to appoint a DPO in your company. Of course, it is recommended to appoint someone (this can be the same person as your AML officer) to monitor compliance with GDPR. Bear in mind that this person will have no specific employment protection as opposed to someone who is appointed as DPO.

22. DO DATA SUBJECTS HAVE SPECIFIC RIGHTS?

The GDPR provides the following rights for individuals:

1. **The right to be informed:** you must provide information explaining that you process the personal data which you have collected in a fair and transparent manner (e.g. through a privacy notice). The information must be (i) concise, transparent, intelligible and easily accessible; (ii) written in clear and plain language; and (iii) free of charge;

2. **The right of access:** the right of access allows individuals to be aware and verify the lawfulness of the processing of their personal data. You must provide a copy of the information free of charge, upon their request. When a request is manifestly unfounded or excessive a reasonable fee can be charged or you can refuse to act on the request. You will need to demonstrate the manifestly unfounded or excessive character of the request;

3. **The right to rectification:** if data is inaccurate or incomplete, the data subject has the right to rectify the data;

4. **The right to erasure** ("the right to be forgotten"): an individual has the right to request the deletion or removal of personal data when there is no compelling reason for its continued processing. This right is not absolute and the request can be refused in certain circumstances (e.g. if the processing is necessary to comply with a legal obligation such as AML or for the exercise or defense of legal claims);

5. **The right to restrict processing:** you will need to restrict processing of personal data in the following circumstances:

   (i) where an individual contests the accuracy of the personal data, you should restrict the

processing until you have verified the accuracy of the personal data;

(ii) where an individual has objected to the processing (where it was deemed necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organization's legitimate grounds override those of the individual;

(iii) when processing is unlawful and the individual opposes erasure and requests restriction instead; and

(iv) if you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim;

6. **The right to data portability:** this right allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. This is most likely not relevant or important for you as a diamond trader;

7. **The right to object:** individuals have the right to object to:

(i) processing based on legitimate interests or the performance of a task in the public interest/ exercise of official authority (including profiling);

(ii) direct marketing (including profiling); and

(iii) processing for purposes of scientific/historical research and statistics.

Diamond traders must in such instances comply with such request and stop processing the personal data, unless:

(i) you can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or

(ii) the processing is necessary for the establishment, exercise or defense of legal claims.

8. **Rights in relation to automated decision-making and profiling:** you can only carry out automated decision-making and profiling in limited situations:

(i) where necessary for the entry into or performance of a contract;

(ii) if you are authorized to do so under national law; or

(iii) if the individual has given explicit consent.

Where such decision-making would occur, you must inform the individual about the processing, introduce simple ways for the individual to request human intervention or to challenge a decision and carry out regular checks to make sure that the automated systems are working as intended.

You are required to respond to such requests **within one month of receipt of the request**. This period of one month may be extended by **two further months** in case of complex or extensive requests.

Note, however, that the above rights are not absolute and that certain restrictions apply in specific circumstances. For instance, you can refuse to act on the request of a data subject if you are unable

to identify the data subject. If the request of a data subject is manifestly unfounded or excessive, you can either charge a reasonable fee taking into account the administrative costs or refuse to act on the request.

There is also a special relation between the GDPR and AML, which affects the rights of data subjects. On the basis of the AML, data subjects do not have the right of access, the right to rectification, the right to be forgotten, the right to data portability, the right to object to processing (including profiling), nor the right to be notified in case of a data breach, in relation to **information that is processed by you in accordance with your obligations under the AML**. As regards the right of the data subject to access his/her personal data that you have processed within the framework of your KYC obligations under the AML, the data subject can exercise this right indirectly via the Belgian Data Protection Authority.

23. WHAT DO I NEED TO DO IN CASE PERSONAL DATA IS STOLEN OR LOST?

The definition of a "data breach" in the GDPR is broad and encompasses the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. It is thus not limited to a malicious attack on the IT systems but can also result from a fault or negligence by a diamond trader's employees.

For example, if one of your employees loses his/her professional laptop which contains personal data, then there will be a data breach. This will also be the case if someone (an employee or any other individual) accesses personal data while he/she is not authorized to do so.

When you become aware of a data breach within your company, you must notify the Belgian Data Protection Authority (www.privacycommission.be) without undue delay and ultimately **within 72 hours** after having noticed the breach. Notification 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 at least state the following:

- a description of the nature of the personal data breach, including the number and categories of data subjects and data records affected;
- the data protection officer's or other contact person's contact details;
- a description of the likely consequences of the data protection breach; and
- a description of how the breach will be addressed, including any mitigation measures taken or proposed.

In addition, when the personal data breach is likely to result in "a high risk to the rights and freedoms of natural persons", you will also need to communicate information relating to the data breach to the data subject without undue delay.

As a diamond trader, you should prepare for this obligation by adopting clear data breach policies which allocate the responsibilities and set out the procedures in case such breach occurs, in order to notify the authorities within the strict timeline imposed by the GDPR. An example of such data breach policy has been prepared by AWDC and can be accessed here.

24. WHICH DOCUMENTS WILL AWDC PROVIDE TO YOU AND HOW TO USE THEM?

AWDC has drafted documents for you, which you can use as templates to use in your company, to ensure compliance with GDPR. A guideline on how to use the templates can be found here. In each question above where any of these documents are of relevance, a reference is made to them, so that you know what they are meant for and what to do with them.

The following documents are made available to you:

- A Guideline on the use of the templates;
- A DPIA questionnaire;
- An external privacy notice to inform your data subjects;
- An employee privacy notice to inform your employees;
- An internal privacy policy to instruct your employees how to handle personal data;
- An example of a confidentiality clause to be included in your employment agreements; (Data protection policy)
- A consent form in relation to your direct marketing activities; (Data protection clause)
- A data breach policy; and
- An example of a general notification in accordance with article 64, §3 AML.

AWDC shall not be liable for any losses or damages resulting from the Q&A or the use of aforementioned documents provided to you.