The 7 greatest misunderstandings about the GDPR

By Menno Loos and Carolin Kaiser

From May the 25th 2018 on, the General Data Protection Regulation (GDPR) is in effect. This EU regulation repeals the Data Protection Directive (Directive 95/46/EC); further harmonising the EU legal landscape on data protection. The Regulation will expand the protection of data subjects and increase compliance duties of controllers, supported by rather serious sanctions.

However, there are still a number of misunderstandings about several subjects and provisions of the GDPR. In this white paper we set the record straight on the 7 most frequently heard misunderstandings.

In the first place, it is not always clear what constitutes personal data. Personal data does not require a name, nor does it only relate to highly sensitive personal information. We will first elucidate this misunderstanding as it determines the applicability of the GDPR. Secondly, we will explain that personal data remains within the scope of the regulation even when it is pseudonymised. Next, the GDPR introduces the duty to maintain a record of processing activities. Many people think this duty only applies to large companies with more than 250 employees. This is the third misunderstanding we will solve. Fourthly, it is often thought that a DPO is the same as a privacy officer, *quod non*. We will elaborate on this and we will discuss the cases in which a DPO must be appointed in your organisation. The fifth misunderstanding concerns privacy impact assessments (PIAs). What is a PIA and when to perform one? In the sixth place, we will discuss covenants. Finally, we will elaborate on the concept of consent.

1. Personal Data
2. Pseudonymisation
3. Record of Processing Activities
4. Data Protection Officer
5. PIA
6. Covenants
7. Consent

1. Personal Data

What constitutes personal data? – is perhaps the most fundamental question in data protection law. Personal data comprises much more than just names, addresses or social security numbers. The GDPR defines personal data as any information relating to an identified or identifiable natural person.[1]
As this definition consists of four elements, it is also known as the four-step test.

1. Any information
2. Relating to
3. An identified or identifiable
4. Natural person

Identifiable
When determining whether a natural person is identifiable, account should be taken of all the means likely reasonably to be used by the controller or by another person to identify the natural person, directly or indirectly. Even if the controller is not able to identify the data subject

[1] Art. 4(1) GDPR, and recitals 26, 27, 30.

by himself, data may still be personal data. For instance, a license plate number constitutes personal data, even if the controller does not have access to the database of the National Road Administration. The mere fact that someone else has access to this database, renders the license plate number personal data.

Identifiable Without Name

It is not decisive whether a name or contact details can be linked to certain information. A person is also identifiable by, for example, the combination of his location and some personal characteristics ("that short girl in the corner"), or other identity characteristics, such as social or cultural identity, belonging to a certain group and being considered a member of it ("that old man of 81 with above-average interest in golf and cigars").

Reasonable Means

Identifiability depends on whether the controller or another person is reasonably able to identify the data subject in the context described above. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs and the amount of time required for identification, taking into consideration the available technology at the time of processing, and (future) technological developments.[2]

Anonymous Data

The GDPR does not apply to anonymous data. Anonymisation is the process of turning personal data into a form which does not identify individuals and where identification is not likely to take place. Data is anonymous when the data subject is not or no longer identifiable. Anonymisation requires more than just omitting names and contact details; the details of 'customer 33' or 'student s849623' are still personal data. Firstly, anonymous data can be obtained by aggregation: this is the compilation of data into information like the average patient with disease X is between 60 and 70. Anonymous data can also be obtained by randomising data. Randomising is the process of randomly interchanging for instance dates of birth and places of residence in a large sample. Between personal data and anonymous data, there is pseudonymised data.

Online Identifier

Natural persons may be associated with online identifiers. Unique numbers such as IP addresses,[3] RFID tags, MAC addresses, or the IMEI numbers of smartphones are often used.[4] These identifiers may serve to link various website visits, recognising a visitor when he or she returns to the website after a previous visit. This is used to create profiles of the interests of natural persons for advertising purposes. The use of such identifiers therefore qualifies as processing of personal data, even if the name of the person behind the identifier is not known.

It may be concluded that the definition of personal data is much broader than is often supposed.

2. Pseudonymisation

In the previous section, we have explained that personal data falls into the scope of the GDPR even when the real name of the data subject is not known. Data relating to a natural person is in

[2] Recital 26, GDPR.
[3] CJEU case C-582/14, *Breyer*.
[4] Recital 30, GDPR.

principle always covered by the GDPR. Only anonymous data fall out of the material scope of the GDPR. But what about pseudonyms?

Pseudonyms

A pseudonym is essentially a person's going by another name than what is printed in his or her passport. Pseudonyms need not even be names as such, but can be any of the (unique) identifiers named in the previous section. In this way, the student number of a university student, the IP address of an internet user, an individual's mobile phone number, or a gamer's user name in an online game may all serve as pseudonyms. Pseudonymous data is therefore the personal data relating to the pseudonymous data subject.

Generating a Pseudonym

Pseudonyms may grant protection to data subjects in some circumstances, but only where they are applied correctly. Most data sets will contain a number of identifiers about a given person. Some of these identifiers will be unique or nearly unique, such as names, dates of birth, or IP addresses. In pseudonymisation, this data is replaced with other information in order to protect the data subject from being identified by these unique identifiers. As an additional safeguard, the GDPR demands that the key to reversing pseudonymisation must be kept separately from the data set itself.[5] It should also be noted that the explicit introduction of 'pseudonymisation' in the GDPR is not intended to preclude any other measures of data protection.[6]

Weakness of Pseudonyms

It is important to realise that pseudonymous data is still personal data. The data subject is still identifiable where information is pseudonymised. For the purposes of the GDPR, it makes no difference if a data subject is identifiable by his or her name or by his or her pseudonym. In addition, pseudonyms are vulnerable to inference attacks. For instance, if a data set of a group of fifty senior citizens is stripped of names, dates of birth, and addresses, the data set will still contain information making each person identifiable. For instance, the data set may contain information about a person's occupation and marital status. Anyone knowing this information about a data subject will thus be able to find and identify that person in the data set.

Using Pseudonyms

Despite these weaknesses, and despite the fact that pseudonymous data is personal data under the scope of the GDPR, the use of pseudonyms may still be attractive for organisations in data processing. By using pseudonyms, the processor may avoid using other identifying information on an individual. This may help the controller to minimise the amount of personal data used in each processing activity, and it may reduce the risk to individuals inherent in such processing activity.

3. Record of Processing Activities

Article 30 of the GDPR describes the obligation to keep a record of processing activities. Controllers as well as processors must maintain an overview of the processing they do. This obligation to keep a record replaces the obligation to notify the supervisory authority prior to a processing.[7]

[5] Article 4(5) GDPR.
[6] Recital 28 GDPR.
[7] Article 18 Data Protection Directive 95/46/EC.

A widespread misconception concerning this record is that the obligation to keep such a record only applies to large companies. This is not true. Smaller organisations may also be subject to this obligation.

The GDPR prescribes that organisations with less than 250 employees are not required to maintain a record of processing activities.[8] However, when one of the following conditions applies, a record is mandatory, regardless of the number of employees.[9]

- Where processing is likely to result in a risk for data subjects;
- Where processing is not just occasional;
- Where criminal records are processed or processing includes special categories of data, such as data about health or religion.

Likely Risk

If an organisation conducts processing that is likely to result in a risk for the data subject, keeping a record is mandatory. To assess whether processing comprises such a risk, the following factors must be taken into account: the nature, scope, context and purposes of processing, as well as the varying likelihood and severity of risks for the rights and freedoms of natural persons.[10]

Not Occasional

Where data is not just processed occasionally, an organisation is obliged to keep a record. An example of an occasional processing is the marketing department informing clients on the change of address after the company moved. This is obviously an occasional processing of the data of the clients. Only processing activities which happen occasionally are excluded from the record of processing activities. Where an organisation processes personal data structurally, it is always subject to the obligation to maintain a record, even if the company has fewer than 250 employees.

Special Categories of Data

In addition, where an organisation processes special categories of data or data concerning criminal records, this processing activity must be recorded. For instance, job applications may contain information on special categories of personal data (passport photo, religious information). Also, when hiring, some companies require a certificate of good conduct from candidates. This information may contain details of a data subject's criminal record. Such data is processed at most undertakings, even small organisations with less than 250 employees.

It can therefore be concluded that most organisations, small or large, do not only process data occasionally. In almost every organisation there is some processing activity that takes place on a structural basis. In addition, it is not uncommon that special categories of data or data on an individual's criminal record is being processed. This results in an obligation to keep a record of processing activity for most organisations, small or large. However, maintaining such a record can also be seen as a measure to get and maintain an overview of the processing activity taking place within an organisation.

[8] Article 30(5) GDPR.
[9] Idem.
[10] Article 30(5), 24(1) GDPR.

4. Data Protection Officer

The GDPR describes different roles in the personal data processing life cycle. One of them is the Data Protection Officer (DPO).[11] The DPO is an independent person within an organisation or within a group of undertakings. His or her main goal is to strive for and monitor compliance with the GDPR. In order to do so, the DPO occupies a special (independent) position,[12] and is assigned several specific tasks.[13]

It is a widespread misunderstanding that a DPO is mandatory for every organisation. It is also not true that a DPO is only mandatory for large organisations. Although it can be very useful for organisations to do so, the appointment of a DPO is only mandatory in three certain cases.[14]

According to article 37 GDPR, a controller or processor must designate a data protection officer in any case where:

1. The processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
2. The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
3. The core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Core Activities

The second and third reason to appoint a DPO refer to 'core activities of the controller or processor'. According to recital 97 of the GDPR the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. According to the Article 29 Working Party[15] these core activities can be considered as the key operations necessary to achieve the controller's or processor's goals.[16] These core activities include activities where the processing of data forms an inextricable part of the controller's or processor's activity. For example, a hospital's main goal is not to process data; it is to provide health care. However, processing data on an individual's health is an inextricable part of health care, it is necessary to provide health care safely and effectively. Health data is one of the special categories of personal data.[17]

These inextricable activities must however be distinguished from necessary support functions for the organisation's core activity or main business. For instance, the HR department of the earlier mentioned hospital may also process sensitive data when it processes cases of sick leave of its own personnel. Such ancillary tasks take place in almost every organisation.

Large Scale

[11] Articles 37-39 GDPR. Another misunderstanding: a privacy officer is not the same as a DPO. Privacy officer is an unofficial definition usually used to indicate someone of the compliance department, charged with privacy. While DPO is a legal definition indicating someone whose position, tasks and responsibilities are laid down in the GDPR.

[12] Article 38 GDPR.

[13] Article 39 GDPR.

[14] Article 37 GDPR.

[15] The Article 29 Working Party is an independent advisory board. See: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

[16] WP243, Guidelines on DPO, p. 7. Accessible here: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048

[17] Article 9(1) GDPR.

The second and third reasons for appointment also speak of a 'large scale' (of monitoring resp. processing special categories). The GDPR does not define what constitutes large scale processing. However, recital 91 does provide some guidance. A large scale processing would include processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects.

As shown above one of the core activities of hospitals is the processing of special categories of data. Since processing also takes place on a large scale, hospitals will generally need to designate a DPO.[18]

In contrast, the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician or other health care professional.[19] Therefore a DPO is not mandatory in these cases.

Between these examples, there is a large grey area which is difficult to classify. The Article 29 Working Party recommends that the following factors be considered when determining whether the processing is carried out on a large scale: the number of data subjects concerned, volume of data and/or range of different data items, duration, or permanence, of the processing; and the geographical extent of the processing.[20]

Appointing a DPO Voluntarily

If an organisation is not obliged to appoint a DPO under the GDPR, it may still do so voluntarily. The Article 29 Working Party encourages such voluntary appointment. It should be noted, however, that voluntary does not mean non-committal. A DPO who has not been appointed to meet an obligation must comply equally with the same rules and frameworks as a DPO whose appointment is mandatory. Having a DPO in-house, whether mandatory or appointed voluntarily, can bring several advantages to an organisation, for example:

1. The DPO can act as an independent supervisor for compliance and as a direct point of contact for the supervisory authority;
2. The DPO may be a point of contact for data subjects in exercising their rights vis-à-vis the controller;
3. The DPO can act as an intermediary between different stakeholders;
4. The DPO can have a supporting role in the execution of (Data) Privacy Impact Assessment ((D)PIA) and advise on the risks of data processing;
5. In the event of an audit or demonstration of the level of accountability, a DPO can relieve an organisation of its responsibilities.

5. PIA

The GDPR introduces the data protection impact assessment, often referred to as a

[18] On the basis of article 37(1) sub c GDPR.

[19] It should be borne in mind that this recital deals with PIAs. This implies that some elements might be specific to that context and do not necessarily apply to the designation of DPOs in the exact same way.

[20] WP243, Guidelines on DPO, p. 7-8. Accessible here: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048
These factors are quite obvious. WP29 provides for some examples in his guidelines. See p. 8.

privacy impact assessment (PIA).[21] It is often thought that such PIA refers to an assessment of a whole company, as some sort of audit to check the overall privacy compliance of a company. However, this is not what a PIA aims to assess. A PIA pertains to defined processing activity carried out by an organisation. Where a type of processing is likely to result in a high risk for natural persons, the controller shall, prior to conducting the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. Where several processing operations are similar and the risks are comparable, it is permitted to cover them in one PIA.[22]

Increased Risk

The standard of a likely increased risk is an open standard. Article 35(1) GDPR stipulates that processing using new technologies is likely to involve an increased risk as the impact of such processing is difficult to estimate in advance. Paragraph 3 of article 35 GDPR lists some examples of situations associated with a likely increased risk: automated decision making, large scale processing of special categories of personal data and large scale monitoring of the public. More generally, recital 91 adds that situations in which processing renders it more difficult for data subjects to exercise their rights constitute an important factor in determining whether processing activity constitutes an increased risk.

Three-Step-Test

Whether a PIA is necessary can be determined in three steps. For each processing, the controller must make an initial assessment of the risks that may exist. If it follows that there is likely to be a high risk associated with a processing, an extended PIA must be carried out. If, subsequently, this shows that the high risk cannot be reduced by reasonable means, the Data Protection Authority (or Supervisory Authority) must be consulted prior to the processing.[23]

6. Covenants

A covenant is a document in which parties declare their intention to work together towards a certain (policy) objective. Usually a covenant, or gentleman's agreement, is an agreement between a number of public and/or private entities. For example, a municipality and a housing corporation may sign a covenant in which they agree to exchange personal data in order to fight nuisance. What is often erroneously assumed is that this exchange (i.e. processing) of personal data is lawful *because* the two parties agreed to do so in a covenant. However, the mere agreement in the covenant does not form a lawful basis for processing. The misunderstanding here is really about lawfulness of processing.

Lawfulness

The first principle that must be borne in mind when processing is that personal data shall be processed lawfully.[24] Article 6 GDPR sums up the six grounds for lawful processing (consent, necessary for the performance of a contract, necessary for compliance with a legal obligation, necessary to protect vital interests of a natural person, necessary for a task in the public interest, necessary for legitimate interests of the controller or third party). Processing shall be

[21] Article 35 GDPR.
[22] Article 35 GDPR.
[23] Article 36 GDPR.
[24] Article 5(1)(a) GDPR.

lawful only if and to the extent that at least one of these grounds applies. A covenant is not one of these grounds and can therefore not form the basis for lawful processing.

We return to the example of a covenant on the exchange of personal data in the context of preventing nuisance. Such practice may be perfectly lawful. However, the lawfulness of the exchange is based on another ground (one of the six above-mentioned grounds); not on the covenant itself. In this case, the lawfulness of processing is based on the necessity for a task in the public interest.[25] One of the tasks in the public interest of the municipality and housing corporation is to – in short – prevent nuisance.[26]

The parties to the covenant must state the legal grounds in the covenant. And where a covenant relates to exchange of personal data, usually the rules on the exchange are elaborated in an attached protocol.

7. Consent

It is sometimes thought that personal data may only be processed after obtaining the consent of the data subject. However, consent is only one of the grounds for lawful processing. As mentioned earlier, article 6 GDPR sums up the six grounds for lawful processing (consent, necessary for the performance of a contract, necessary for compliance with a legal obligation, necessary to protect vital interests of a natural person, necessary for a task in the public interest, necessary for legitimate interests of the controller or third party).

Obtaining Consent

Consent should be a freely given, specific, informed and unambiguous indication of the data subject's wish, signifying agreement to the processing of his or her personal data.[27]

Where processing is based on consent, the controller should be able to demonstrate that the data subject has consented to processing of his or her personal data.[28] The proof that permission has been obtained is free of form. Well-known ways to prove consent are a signed written statement, an online check mark that must be checked before proceeding, or a recorded oral statement. In practice, generic proof is often used, as in the case of the online check mark: it is then proved that the system on the day in question worked in such a way that permission was required to proceed, from which it follows that the data subject also gave permission.

Children

Article 8 GDPR describes the conditions applicable to consent in relation to information society services where children are concerned. If the child is below the age of 16, processing is only lawful if and to the extent that consent is granted by the child's parents. However, the GDPR leaves some space for deviation by Member States. Member States may lower the age limit of the GDPR for those purposes,

[25] Article 6(1) sub e GDPR. To be able to use this legal basis it must be established that the processing of personal data is in fact *necessary* in order to perform the task in the public interest.

[26] These tasks are laid down in national law. In the Netherlands the mayor is responsible for maintaining public order (art. 172 Gemeentewet). Housing corporations have the task to contribute to the viability in the area of their residential units (art. 45(2) sub f Woningwet). However, even for this task personal data may only be processed in so far as is necessary.

[27] Article 4(11) and recital 32 GDPR.

[28] Article 7(1) GDPR.

provided that such a lower age is not below 13 years.[29]

Sensitive Data

Finally, article 9 GDPR describes the grounds for processing special categories of personal data (sensitive data). Where consent is given for the processing of sensitive data, consent must be explicit. When granting consent for the processing of personal data that do not fall into special categories, it is possible to infer implied consent based on the data subject's conduct, as long as it is clear that the data subject has consented to the proposed processing. Consent for the processing of special categories of personal data requires more: there must be an explicit expression of the deliberate intention of giving consent. The threshold for giving consent for sensitive data is therefore higher than for personal data.

[29] The Netherlands do not deviate from this age. The Dutch Act implementing the GDPR, like the earlier Dutch Data Protection Act, keeps the age of 16. Conf. point 4.11 of the Dutch Act implementing the GDPR and article 5(1) of the Dutch Data Protection Act.