WHITE PAPER

The GDPR, what does it mean for non-EU companies?

DPO Consultancy
Experts in Data Privacy

DECEMBER 2020

Introduction

What kind of measures do organizations from outside Europe need within the context of privacy and data protection, when deciding to do business in Europe? One key aspect is the GDPR or General Data Protection Regulation. But when your company is not located in the European Union, why should the GDPR apply to you? This is an interesting question that we will discuss in this white paper. Looking from a distance it seems obvious that when you are, for example, based in the United States, you are not captured by the GDPR, since you are not a European company. But is this really true? The answer, like many in the field of law is: It depends.

Often, we are confronted with the misconception that European law is only applicable to citizens and organizations located in Europe. Although this is understandable, the applicability of the GDPR is more complicated. Under certain circumstances you can be captured by the GDPR, even when you are based abroad. It largely depends on the kind of relation you have with Europe and individuals in Europe. For example, if you offer products or services to individuals in Europe you will have to comply with the GDPR, even when you offer these products or services over the internet. In certain circumstances you will even be obliged to appoint someone in Europe to be a representative (a Data Protection Representative or DPR) for your company.

The GDPR, like many other laws, has a certain territorial scope. The territorial scope of the GDPR reaches further than just the European continent and can even be applicable to companies established outside the European Union, or to people that do not have European residency or citizenship. One of the European Union's key principles is the protection of the rights of individuals. This protection extends from inside the EU to outside of the EU. Comparable with personal data that is transmitted borderless through the internet, the protection of individual rights under the GDPR is also considered to be more or less borderless. This means that for a non-EU organization that has a small engagement with individuals located in the EU, the GDPR has full effect, also with regards to fines. This has implications for many companies, as they might have to appoint a Data Protection Representative (DPR) and/or a Data Protection Officer (DPO) in Europe, even when they are not located within Europe.

How this all works is what we will explain in this white paper.

By the end of 2020 we will know what happens to the EU – UK relationship. On December 31st 2020 both parties should decide how the relationship will work. Currently there have been little concrete solutions proposed when it comes to the GDPR. It is still a real possibility that the UK will leave the European Union with a no deal scenario. What this could mean for GDPR responsibilities is summarized in chapter 4 of this white paper.

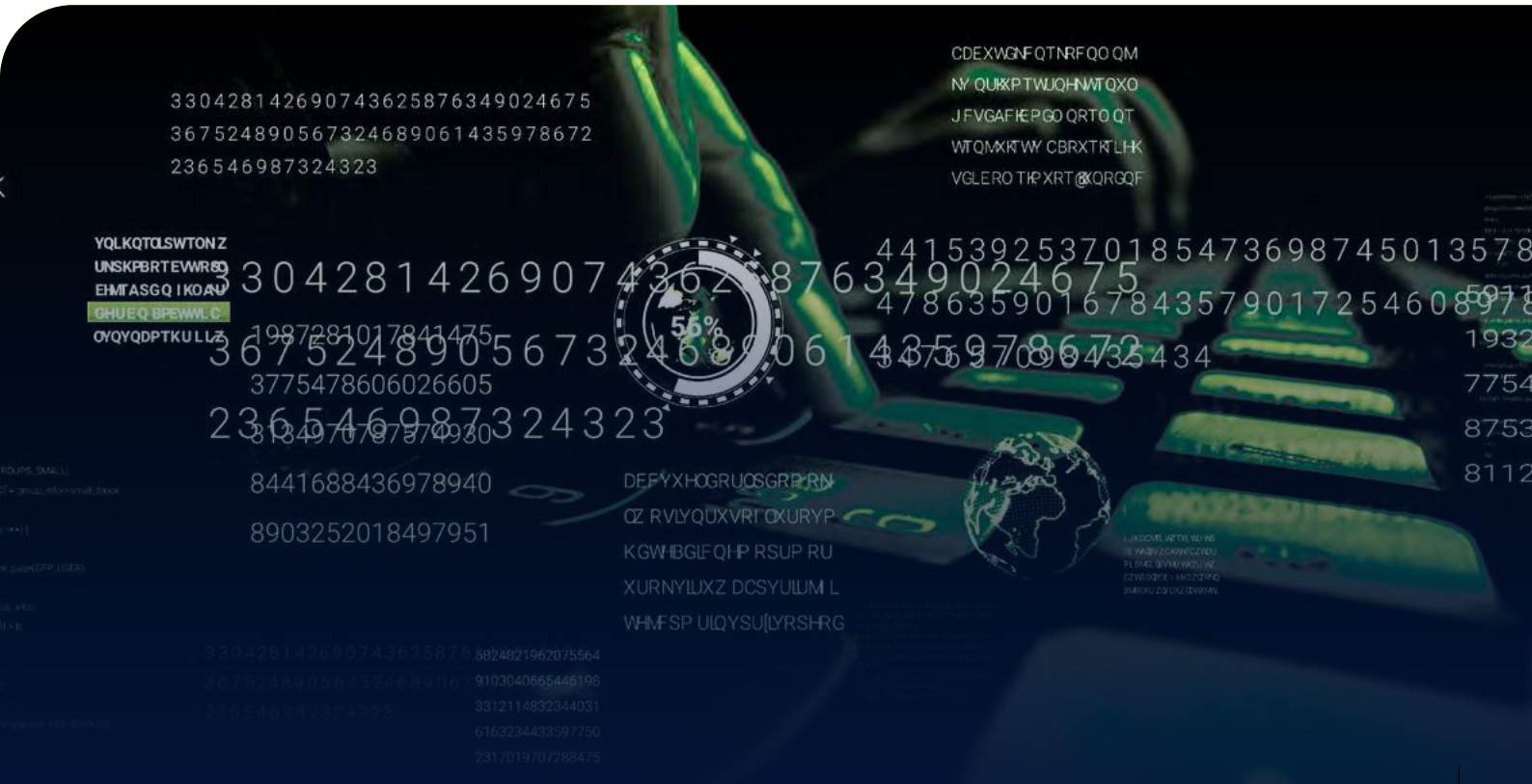
1. The scope of the GDPR

The GDPR has a material scope and a territorial scope. The material scope defines when the GDPR comes into effect and when it does not. Basically, this explains when it is applicable and when it is not.

When talking about processing of personal data, as a rule of thumb we can say the GDPR is in effect **unless** any of the following situations are applicable:

- when processing of personal data occurs in the course of a household activity by natural persons,
- when processing occurs in a national and / or union security, police and counter terrorism setting,
- when processing happens by EU bodies (a separate act comes in to play here),
- partly when processing is done by internet service providers.

Like many laws, the GDPR also has a territorial scope. This means that the law is meant to have an effect on certain people or a certain area. When talking about the GDPR, we are talking about European legislation,



meaning the GDPR is applicable to all EU citizens and people within the European Union. That makes sense, but what is often overlooked is that the GDPR also reaches beyond the European borders and can have an effect outside Europe, and on non-Europeans. What does this mean? Let us examine.

Establishment

Firstly, when an organization established outside the EU opens an office inside the EU and starts delivering goods and /or services (read: processing personal data) to individuals in Europe, the GDPR applies. An example would be an American web shop that, while established outside the EU, offers American made goods to European customers. According to the European Data Protection Board, establishment means a degree of stability in the arrangement and the exercise of activities in the European Union. In other words, there must be a clear link between the personal data that is being processed and the activities of the establishment in the EU. Having a third-party process personal data on your behalf within the EU (in the GDPR we call this a "processor") does not in itself constitute an establishment and does not directly mean that the GDPR applies to the organization. Just having a website in the European Union does not mean that the GDPR is directly applicable to the organization. However, having a website to support the processing of personal data in the European Union could mean that the GDPR applies to the organization.

Applicability outside of European borders

Secondly, the GDPR is also applicable outside of European borders, when personal data of individuals in Europe are processed outside Europe. For example, even though an American organization only has a website and

"The GDPR applies, even when this American organization has no physical presence in Europe."

no office in Europe, but is indeed processing personal data from Europeans, the GDPR applies. Even when this American organization has no physical presence in Europe.

Monitoring and tracking of individuals in Europe

Thirdly, the GDPR applies when individuals within European borders are being monitored or tracked (being targeted) by companies outside of Europe. For example, by placing cookies while Europeans visit websites that are located outside of Europe. When an individual visits Facebook, this organization can place tracking cookies on that individual's laptop or smartphone to track and monitor their behavior in order to show them relevant and personal advertisements.

Applicable to everyone in the EU

Lastly, the GDPR applies to persons who are located within the EU. This means it is not relevant whether or not an individual has his or her citizenship or residence in the European Union. For example, individuals who pass through the EU on their way to another destination outside the EU are subject to the GDPR.

What is outside the territorial scope of the GDPR?

When Europeans are visiting other countries outside European borders, for example when on holiday, they can be tracked and monitored according to local laws. When someone visits the United States, their personal data may be processed according to anti-terrorist legislation. This falls outside the scope of the GDPR.

What does this all mean for non-EU organizations operating in Europe?

In general we can state the following: the GDPR applies to all non-EU organizations, operating in Europe in case they:

- Have established a European office and are processing personal data from persons residing in Europe.
- Are conducting business in Europe without a physical presence.
- Processes personal data coming from individuals in Europe in any other way.

When one of the situations described above applies to your organization, you might need to appoint a Data Protection Representative (DPR). It is safe to state that if your organization is systematically (regularly, so not on an occasional basis) processing personal data, coming from individuals residing in the EU, you need to appoint a DPR. This is because when the processing is done systematically by the organization, there is a clear and obvious focus on Europeans and the European market, which makes the GDPR applicable.

2. Reasons to appoint a DPR

"The GDPR is not a one-off piece of legislation that will fade out of focus as time passes."

A risk based approach is often a good approach. But while this is a strategy employed by some companies, it is becoming clearer that the GDPR is not a one-off piece of legislation that will fade out of focus as time passes. The GDPR will not only become clearer as times passes, more specific legislation is currently being developed as we speak. In addition to more specific regulation, we are noticing that the European Court of Justice is increasingly supporting the rights of individuals with regard to ownership, and control of their personal data.

More and more fines are being issued to companies that do not comply with the GDPR, in part or in whole. Relevant to the appointment of a DPR is the 2015 "WhatsApp" case. The Dutch Data Protection Authority concluded that WhatsApp must appoint a DPR in the Netherlands within three months, or otherwise face a penalty of €10.000 per day with a maximum of €1.000.000. WhatsApp stated that a DPR cannot be seen as a controller in the EU and that this would be inconsistent with the Data Protection Directive, in part or in whole. Furthermore, it stated that in this specific case it would be preferable to wait until the GDPR would come into effect. The court did not agree with WhatsApp and confirmed the fine by the Dutch Data Protection Authority.

In addition to complying with legislation, there is another appealing aspect for organizations to comply with the GDPR by appointing a DPR. Protecting the data of the organization's (European) customers can be a substantial benefit to the organization when seeking to acquire and retain customers' trust. Customers are increasingly conscious of how their data is being used by companies and what recourse they might have under the GDPR. By complying with the GDPR, the organization is proactively showing that it respects the privacy and the personal data of its customers.

3. The Brexit question

When the United Kingdom leaves the European Union on a no-deal scenario this will have implications when looking at data transfers to and from the United Kingdom and the European Union, and what needs to happen when looking at a DPR. As we speak, the privacy law in the United Kingdom is virtually the same as in the European Union. This is because the GDPR was transposed into English national legislation. This may however change over time as of the 1st of January 2021 the United Kingdom no longer implements European legislation.

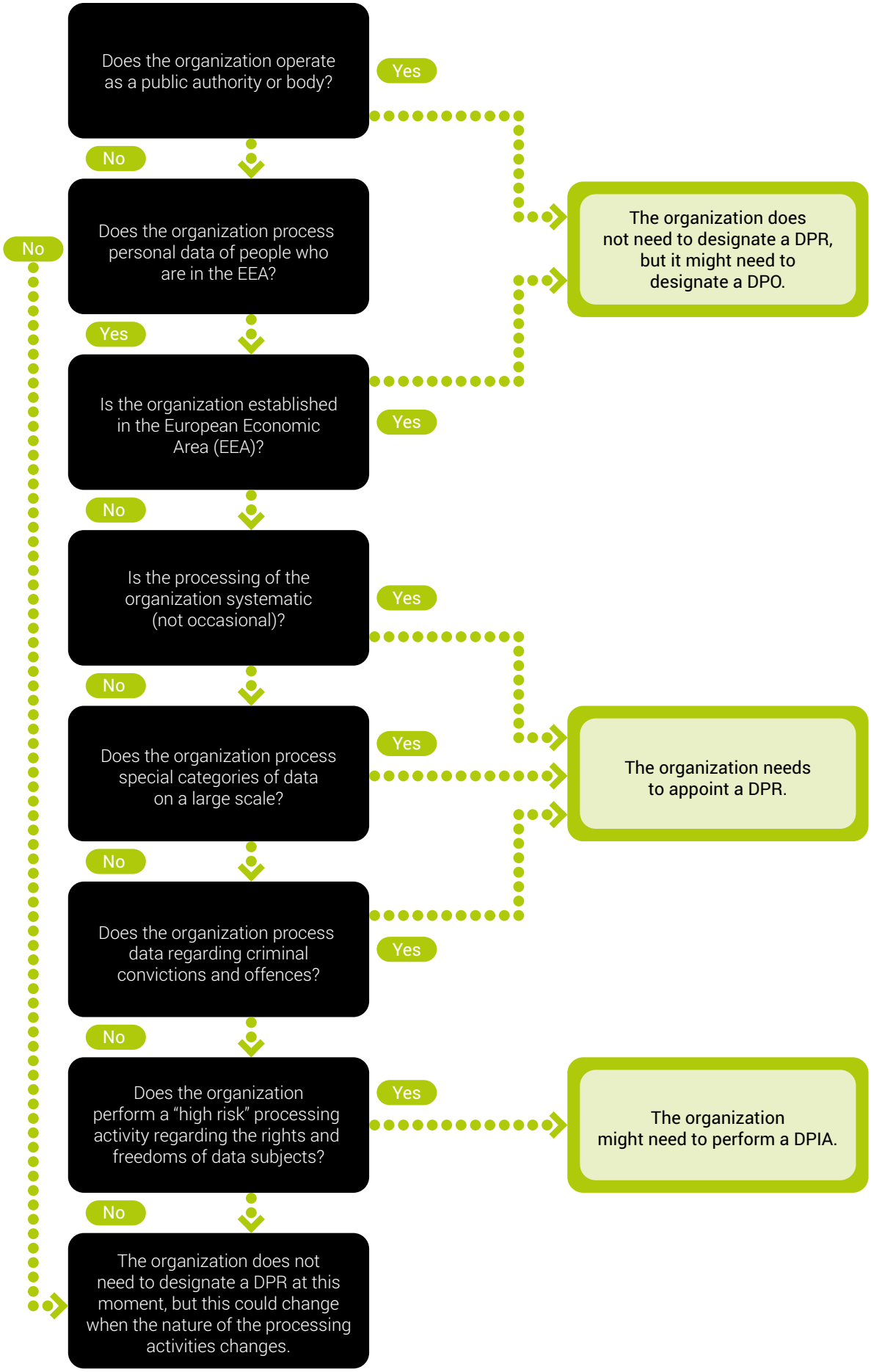
The English Data Protection Act can be changed. The United Kingdom currently considers the European Union an adequate country under the Data Protection Act, but the European Union has not reciprocated this. The recent Schrems II ruling on government surveillance and data transfers in the United States is certainly impacting this decision. A similar situation could arise in the United Kingdom. If Brexit happens on a no deal scenario, what happens to the DPR obligation?

You are a data controller outside the European Economic Area (EEA), processing data from the UK, the EEA or both.
When you focus on the EEA market and the UK market, and you are based outside both jurisdictions, you need to appoint a DPR in both countries. The reason for this is that the Data Protection Act is a translation of the GDPR and under both separate legal regimes, the same obligation exists.

"If Brexit happens on a no deal scenario, what happens to the DPR obligation?"

You are a data controller in the UK, processing data from the EEA.
When you focus on the EEA market and you are a UK based organization. You need to appoint a DPR in the EEA, meaning someone located in the EEA that meets the criteria of being a DPR under the GDPR.

You are a data controller in the EEA, processing data from the UK.
When you focus on the UK market and you are a EEA based organization. You need to appoint a DPR in the UK, meaning someone located in the UK that meets the criteria of being a DPR under the Data Protection Act.


Does the organization operate as a public authority or body?
Yes
No
Does the organization process personal data of people who are in the EEA?
No
Yes
Is the organization established in the European Economic Area (EEA)?
Yes
No
Is the processing of the organization systematic (not occasional)?
Yes
No
Does the organization process special categories of data on a large scale?
Yes
No
Does the organization process data regarding criminal convictions and offences?
Yes
No
Does the organization perform a "high risk" processing activity regarding the rights and freedoms of data subjects?
Yes
No
The organization does not need to designate a DPR, but it might need to designate a DPO.
The organization needs to appoint a DPR.
The organization might need to perform a DPIA.
The organization does not need to designate a DPR at this moment, but this could change when the nature of the processing activities changes.

4. What does it mean to have a Data Protection Representative?

What is the role of the Data Protection Representative within an organization? A DPR is the organization's representative in the EU, its Data Protection Authorities, and for the individuals whose personal data is being processed (data subjects). A DPR acts in the organization's name, and partially lays down this obligation because of practicality. It is not hard to imagine that it can be quite difficult for an individual to come into contact with a foreign entity. This also accounts for contacting Data Protection Authorities in the EU itself. Communication will be a lot smoother when there is a permanent representative. The DPR can be both a natural or a legal person.

What is the role of DPR?

The DPR has insight and access to the details regarding the processing of personal data that is carried out on individuals in Europe by the organization. Meaning that the DPR needs to have access to the organization's overview of personal data that is being processed. In the GDPR this is called the 'record of processing activities'. Furthermore, the DPR also needs to have access to relevant procedures within the organization in order to act in its capacity as the representative. For example, when an individual informs the DPR that he/she wants to receive a copy of the personal data that is being processed about him or her, the DPR needs to be able to help the data subject with regard to that request.

"The DPR does not carry full legal responsibility for the processing of personal data."

Responsibility

The DPR does not carry full legal responsibility for the processing of personal data. This responsibility remains with the organization that determines the purposes and means of the processing of personal data outside the EU. In the GDPR we call this the 'data controller'. However, the DPR can be held partially liable in certain aspects regarding the GDPR, such as how he or she carries out his role as DPR and can be subject to enforcement procedures.

"A DPR needs to be a natural or legal person residing in a member state of the European Union."

Location

The most ideal location for assigning a DPR is in the country where most of the targeted individuals are located. This stimulates and ensures a smoother communication. However, it could be the case that international organizations who are processing personal data from data subjects across multiple countries, must appoint a DPR. In this case appointing one DPR is enough, as long as there is proper infrastructure in place for communicating with data subjects from all relevant countries. This means that communication to the data subject must be in his or her own native language.

Is it possible to combine the function of a Data Protection Officer (DPO) and the DPR?

Both functions cannot be combined. This results from their respective different positions and tasks. A DPO is responsible for oversight of the data privacy management within an organization. A DPR is a contact person for data protection authorities in the EU, and its data subjects. Additionally, the European Data Protection Board has issued a further statement that clarified that there is a potential conflict of interest between a DPR and a DPO[1].

How to appoint a DPR

A DPR needs to be a natural or legal person residing in a member state of the European Union. If your organization has an office in one of the European member states it makes sense to install a DPR there. Often the best choice is to appoint an experienced, independent person or legal entity outside of your company, as this guarantees impartiality and prevents a conflict of interest.

Keep a close eye on where most of your data subjects are located. If most of them are located in a certain member state, make sure that your DPR speaks the language of those data subjects. A legal background is certainly required as your DPR is exposed to certain risks and so is your organization. Make sure that your DPR is in direct contact with the organization outside the European Union. The DPR will be the first point of contact for member states, data protection authorities and people and organizations with legal discourse. The DPR will need to have access to systems and databases (or instruct people with access) in order to fulfill data subject access requests and maintain the record of processing activities.

Closing remarks

As we have seen the territorial scope of the GDPR reaches further than many other European laws. It aims to fully protect the rights of data subjects residing in the EU, who are being targeted by the processing activity of an organization. It can have implications for organizations that are not located in the EU, and for people with no European citizenship or residency. A far-reaching piece of legislation to say the least.

An important aim of the GDPR is to level the playing field when it comes to data protection legislation, hereby fostering economic growth and development. This may result in far-reaching consequences for non-European companies trying to establish themselves within the European market. For these organizations, this often means the mandatory appointment of a Data Protection Representative. While this might seem like a challenge, it offers great benefits for organizations. It often means smoother communication between the EU, its member state authorities, and the relevant individuals.

With increasingly more pro-active national data protection authorities and a European Court of Justice, appointing a DPR is no longer only legally the right thing to do, it is also a way for an organization to proactively show their commitment to GDPR compliance, meaning that they also reassure their customers their personal data is in great hands, while other companies might fall behind on this promise.

DPO Consultancy
Experts in Data Privacy

Australiëlaan 12a
5232 BB 's-Hertogenbosch
The Netherlands

Congresstraat 35
1000 Brussels
Belgium

1 Lyric Square London
W6 0NB
England

+31 850 711 080
info@dpoconsultancy.nl
www.dpoconsultancy.com