Deloitte.

The General Data Protection Regulation

Long awaited EU-wide data protection law is now applicable

Introduction

May 25th... A defining day in Privacyland. As I write, the long-awaited introduction of the General Data Protection Regulation is upon us. And what a busy time the run-up to this day has been! My team has been supporting many, many organisations as they geared up their data policies and practices to comply with GDPR. From performing gap assessments and running transformation programmes to advising on governance issues. I am really proud of my team and what we have achieved together.

Tried, tested and new
A snapshot of organisations today would show varying degrees of GDPR-readiness. Some are very well prepared, but there is room for surprises, as we do not know how exactly GDPR will be enforced in practice. Some organisations still have some ground to cover. And there are some still at the very start of their journey. Deloitte will continue to provide them all with our tried and tested GDPR services.

But we are now entering a new reality for organisations, with new needs. And Deloitte is ready to respond. One new factor is regulatory enforcement: organisations must deal with questions from supervisory authorities on their handling of personal data, and may even see inspectors visit their premises. Deloitte now has a rapid-response team on hand to help them.

Reaping the benefits
But the compliance side of things is just part of the story. Deloitte is equally focused on the opportunities that GDPR brings. The real emphasis of our new services, therefore, is on helping organisations reap the benefits of their data.

The new regulations have forced organisations to create order in the information they have. And order provides insight. Insight into value that was hidden there. Deloitte is here to help organisations explore the business potential of their data sets, and be their partner in new ventures. Could privacy excellence even become an organisation's Unique Selling Point?

Catching up
In the past year, through articles, blogs and vlogs, our team has shared a vast amount of relevant information with the public on privacy-related issues. We have now brought them together in this magazine, as an easy way for our clients to catch up. But developments do not stop here, nor will we. I am really looking forward to the next season in Privacyland!

Annika Sponselee

Annika Sponselee is Deloitte's Global Solution Leader for GDPR and the Hub leader for GDPR in North-West Europe (Netherlands, Belgium, Switzerland , UK, Ireland and the Nordics), where Deloitte has 150 dedicated privacy professionals. In the Netherlands, she heads a team of over 25 seasoned experts with legal, security, IT and compliance backgrounds.

The General Data Protection Regulation (GDPR) promises data protection rules that will remove red tape for businesses but also tighten privacy protections for online users.

Content

The General Data Protection Regulation

Long awaited EU wide data protection law finalised

The General Data Protection Regulation (GDPR). It has been in the making for over four years but in April 2016 it was finally finished. The regulation promises data protection rules that will remove red tape for businesses but also tighten privacy protections for online users.

What is the GDPR?
Since the mid-1990's, legislation that protects the information privacy of individuals in the European Union (EU) has been primarily based on EU Directive 95/46/EC: the Data Protection Directive. This is the legislative act that has set out the minimum standards on data protection in the whole of Europe. Each country within the EU has taken Directive 95/46/EC and transposed it into their own, local data protection laws. The Dutch Wet bescherming persoonsgegevens, German Bundesdatenschutzgesetz, Belgian Privacywet / Loi vie privée and United Kingdom's Data Protection Act 1998 are all examples of such local laws.

Since the Directive has essentially not changed since 1995 and all local legislation based on it has only seen minor updates, the European Commission and European Parliament deemed it outdated to meet modern privacy needs and concerns. Therefore preparations have been started over four years ago to come up with a replacement A European data protection act that is up to date and protects individuals' privacy in the digital world we live in today.

That data protection act has now been finalised. It is called the General Data Protection Regulation (GDPR) and will replace local data protection laws, such as the ones mentioned above, being valid in every country of the EU. The EU institutions made good on their promises to remove red tape for businesses but also tighten privacy protections for individuals. This means privacy rules will change and organisations that deal with information relating to individuals will need to adept.

Significant changes in privacy rules
On this page we describe a number of these changes, the ones we feel will have the most impact. The complete GDPR is over two hundred pages in length, so what follows is a very brief summary and not meant to be an exhaustive list. Please refer to the official text as authoritative source.

Data portability
The GDPR strengthens the rights that individuals have to control their own data. One of the most significant examples of this is a new right that has been granted to individuals: The right to data portability. It basically says that an individual has the right to transport his personal data from one organisation to the next – hence the word 'portability'. The personal data must be provided to the individual in a structured, commonly used and machine-readable format. And the rules also stipulate that when technically feasible, organisations should facilitate electronic transfer of personal data from one to another, if the individual requests this.

Inventory
The legislators have made good on their promise to remove red tape, as the obligation to notify local authorities of personal data being processed, is gone. This has for a long time been seen as a difficult and rather bureaucratic rule, putting a large burden especially on internationally operating organisations. However, in its place a rule has been created that an organisation now must maintain a record of processing activities under its responsibility – or, in short, that they must keep an inventory of all personal data processed. The minimum information of what should be in the inventory has been described and it goes beyond just knowing what data the organisation processes. Also included should be for example the purposes of the processing, whether or not the personal data is exported and all third parties receiving the data.

Data protection by design and by default
Data protection by design and by default are both included in the GDPR. This basically means two things. First, it will be mandatory when designing a new system, process, service, etc. that processes personal data, to make sure that data protection considerations are taken into account starting from the early stages of the design process. Moreover, organisations need to be able to prove that they have done so. Second, when the system, process, service, etc. to be designed will include choices for the individual on how much personal data he shares with others, the default setting is the most privacy friendly one, so the one that says to not share any information at all. This data protection by default notion further includes data minimisation principles.

Expanded territorial scope
Interesting to see in the GDPR is the notion of territorial scope. This states that the GDPR (and therefore the European privacy laws) also applies to organisations that are not located within the EU, but that do offer goods or services to, or monitor behaviour of data subjects in the EU! In other words, organisations that target EU residents via the internet with services, goods or for monitoring, have to be compliant with EU rules on privacy of those residents' data. It looks like this creates an interesting precedent, where the rules follow the data instead of being strictly territorial.

Processors
If you are processor (you process personal data on behalf of another organisation), the GDPR has a significant change for you in store. Where so far all the burden of compliance with privacy legislation was on the controller (your client), now you get some obligations yourself directly as well. You will get responsibilities directly under the law and will be accountable as well. Some of these new responsibilities include that a processor must appoint a Data Protection Officer and keep records of all their processing activities they perform on behalf of clients. Moreover, a supervisory authority can go to processors directly with requests and demands. It is to be expected that this will shift the balance of power between controllers and processors to a more equal playing field.

Right to be forgotten
Another data subject right that already got a lot of attention the past years is the right to be forgotten. The data subject's right to erasure of his personal data did already exist in the current Data Protection Directive but is now elevated in the GDPR. Under the new regulation all organisations that process personal data must remove all of that data if one condition (out of a list of six) is met. The list of conditions includes when it is clear that data have been processed unlawfully and the case when a data subject withdraws previously given consent. This 'new' right received a lot of attention due to the Google v. Spain case in which the Court of Justice of the European Union ruled in accordance with this new obligation.

PIAs
The GDPR introduces Data Protection Impact Assessments (DPIA) as a means to identify high risks to the privacy rights of individuals when processing their personal data. When these are identified, the GDPR expects that an organisation formulates measures to address these risks. This assessment should happen prior to the start of processing the personal data and should focus on topics like the systematic description of the processing activity and the necessity and proportionality of the operations. With that the DPIA resembles Privacy Impact Assessments (PIAs) that many organisations already execute regularly. The contents of PIAs however was never strictly defined, so perhaps this helps in getting more uniform assessments.

Security
The need to take proper information security measures to ensure the confidentiality, integrity, availability and resilience of processing systems and services has always been a part of privacy legislation. New is that the GDPR champions pseudonymisation and encryption of personal data: These security measure are thought so valuable that they have been specifically mentioned in the text of the act. Furthermore it is stressed that security should be based on a risk assessment, however not of the risks the organisation faces, but the risks for the rights and freedoms of natural persons, i.e. the risks that an individual's privacy is compromised.

Accountability and data governance
Data protection legislation in the EU has always been based on a number of principles that need to be adhered to. Lawfulness, fairness, purpose limitation and transparency are well known examples of those. The GDPR introduces a new principle: accountability. Organisations will not only be responsible for adhering to all the principles, they also must be able to demonstrate compliance with them! For most organisations this means they will have to elevate their internal privacy governance maturity, not only because of this new accountability principle but also because the public opinion will expect it from modern organisations.

Sanction
One of the most discussed aspect of the GDPR must be its explicit mentioning of fines. Whereas the Data Protection Directive only had one line stating that sanctions had to be defined by the Member States, the GDPR exactly details what administrative fines can be incurred for violating articles of the GDPR. The maximum fines depend on what the "category" in which the violation occurs: For less serious violations, the maximum is € 10 million or 2% of total annual worldwide turnover of the preceding year (whichever is higher); for more serious violations this goes up to € 20 million or 4%.

One stop shop
As a partial relief for organisations that operate across the EU, a sort of 'one stop shop' system for supervisory authorities in Europe will be introduced. The GDPR introduces a co-operation system between supervisory authorities. The 'Lead Supervisory Authority' will be the supervisory authority of the country in which the data controller or processor has its main establishment. The Lead Supervisory Authority will be the primary authority organisations need to deal with, but under circumstances local authorities can step in as well. They need to co-operate, but it will be interesting to see how this co-operation will function in practice.

Approved certification mechanism
The legislators have acknowledged that for many organisations being able to proof that they adhere to the GDPR will be an advantage. For that purpose data protection certification mechanisms and data protection seals and marks are introduced. The GDPR even speaks about the possibility to come to a common European Data Protection Seal. And although for now the GDPR provides scant details it is to be expected this mechanism for showing adherence will develop in the coming years.

Local deviations
It is critical to note that the GDPR is a Regulation, not a Directive. Where the Directive 95/46/EC was transposed into local laws in each European country the GDPR, as EU Regulations go, will be directly valid. This will be a relief to many organisations that operate in multiple countries within the EU – having to account and comply with slightly different rules on data protection in each EU member state can be a legal and operational nightmare. However, we do note that in the GDPR the legislators have provided local governments the ability to add or adept provisions to fit their local data protection needs. Views on how much individuals' personal data should be protected and from whom are deeply rooted in local culture. Even within the EU vastly different opinions exist on this from one country to another. It is expected that that many governments will make provisions in line with local cultural habits and views.

Next steps for any organisations now that the final text of the GDPR is known, is to identify how this new legislation may impact them. This will of course vary per organisation, but in general terms, privacy consists of making sure you address not only the legal aspects. This new regulation emphasises that it is also about making sure that you have organised yourself properly to deal with privacy and you have the technical ability to do so.


STARK Lock
Bestguard
TRI-MOON
Bestguard
EXCEL
YETI

The GDPR: Areas of Attention & Practical Guidance

Where to start when becoming GDPR and e-Privacy compliant?

This blog indicates specific areas of attention and includes practical guidance of where to start in becoming GDPR and e-Privacy Regulation compliant.

By this time, most companies are aware that the GDPR and the e-Privacy Regulation, which is currently under negotiation, will bring significant changes to the privacy landscape. Translating the regulation's theoretic contents into a practical implementation that fits the business, will be a major challenge for many organizations. This blog will indicate specific areas of attention and includes practical guidance of where to start.

Areas of attention

An important starting point with the GDPR is the concept of personal data. The GDPR is only applicable when personal data is processed. Personal data is data by which a natural person can, directly or indirectly, be identified. Most people are aware that, for example, a name, an address and an email address are personal data. But there is more. Also an IP address or device ID are considered to be personal information.

In addition to that, a distinction is made between 'regular' personal data and 'special categories of personal data'. The last category may include a photo which reveals someone's race or the registration of the reason for an employee's sick leave. Organizations should avoid collecting such data unless one of the exceptions that allows processing applies.

A third complicating factor is that the GDPR also applies when data is indirectly traceable to a person. Data could appear not to be personal data at first sight, but in combination with other data or in a particular context, it can lead to an individual and is thus personal data. This means that the scope of the GDPR is very broad.

Pseudonymized or anonymized data is sometimes assumed not to be personal data.

This could be convenient because it seems that the GDPR no longer applies to this data. Unfortunately, this assumption is incorrect.

The GDPR is explicitly applicable to pseudonymized data.

Pseudonymized data is data of which the most identifying fields within a data record are replaced by pseudonyms. The GDPR does considers pseudonymization as a suitable form of security.

And what about anonymization? If a dataset is anonymized, then the GDPR is no longer applicable. But the bar is set high. The data must be encrypted, the key discarded, and all data that can be redirected to a particular person has disappeared – the encryption has thus been made irreversible. That last criterion is almost never fulfilled. In most cases a dataset contains combinations of data, for it to be useful or interesting. Often it is this combination that can still lead to an individual.

Controller, Processor, Processing and Data Subject

In the GDPR, the controller, processor and data subject are key concepts. The controller determines what happens with personal data and how data are processed. The processor processes the data solely on behalf of the controller. The data subject is the person whose personal data are processed.

Many of our clients have questions about the requirements regarding a processing agreement. Examples of a questions are: When is there an obligation to conclude a processing agreement? When does an organization qualify as a controller and when as a processor?
A processing agreement is necessary when another party is involved in the processing of personal data for which your organization determines the means and purposes. Within the boundaries of that processing agreement, the processor can process the data on your behalf. However, when a processor acts beyond the limits of the processing agreement, it automatically becomes responsible for the processing activity. All obligations arising from the GDPR are then directly applicable to that party. For example, the processor will need a proper basis for processing the data. This can be problematic, especially when it concerns processing sensitive data. In addition this may cause liability for the initial controller.

Data Protection Officer (DPO)
Not all organizations are required to appoint a DPO. A governmental organization, a -large- organization that processes personal data on a large scale, and an organization which is primarily responsible for processing sensitive categories of data are in particular obliged to appoint a DPO. However, the GDPR leaves room for interpretation. When are you considered to process personal data on a large scale, and when are you "mainly charged" with processing of personal data? As for the latter: think of a hospital, for example. The processing of sensitive personal data is a core activity. A company in marketing and advertising wishing to use for example, location data, the appointment of a DPO could be mandatory. A DPO does not necessarily need to be someone from within your organization. It may also be an external person.[4]
assessment, however not of the risks the organisation faces, but the risks for the rights and freedoms of natural persons, i.e. the risks that an individual's privacy is compromised.

e-Privacy Regulation
In addition to the GDPR, the e-Privacy Regulation will also bring a lot of changes. The draft Regulation is currently going through the EU legislative process. The ambition is that this Regulation will become enforceable at the same time as the GDPR, in May 2018. The question is whether this is ambition is a realistic one.

The current e-Privacy Directive includes rules to ensure the confidentiality of communications (including: the prohibition of interference) and the use of cookies. The current e-Privacy Directive regulates the protection of the right to privacy and is focused on traditional telecom providers, such as ISPs. The e-Privacy Regulation will also focus on "over the top" services (OTTs) such as Whatsapp, Facebook Messenger, Gmail, Skype, and Snapchat, in addition to the traditional providers. This means that these service providers must also ensure the confidentiality of communication by citizens and must prevent disturbance, interception or monitoring. This also applies to machine-to-machine communication and therefore, Internet of Things (IoT) communication is also covered. The reason for the broader scope of the e-Privacy Regulation is that consumers and businesses, in their communications, are increasingly dependent on new Internet services. Phone calls and paper letters are now online phone services and emailing via Voice over IP, instant messaging and webmail services.

In addition to the content of communication, so-called 'metadata' are also protected by the regulation. This includes location data, time and duration of communication and the sender. Using current technology, this data, provides almost as much insight into one's private life as the content of the conversation itself.

Cookies
Many organizations have questions about the changes the e-Privacy Regulation will bring regarding the use of cookies. As it seems now, the Regulation will not necessarily make this use easier.

Cookies may be used when (1) this is necessary for transferring the data, (2) or if it is required to provide the requested services, (3) when it is necessary for measuring web statistics (first party cookies), or (4) when consent was given by the data subject.
For the obtained consent to be valid strict requirements apply. The consent request must be presented in an understandable and easily accessible form and in plain and simple language. In addition, the data subject must be able to withdraw given consent at all times and consent must be given freely. The controller must be able to demonstrate that it obtained consent. If consumers or users do not explicitly give their consent for processing their data, companies must, according to the proposed Regulation, anonymize or delete the data.
Cookies that are necessary for the proper functioning of a website or service and cookies that maintain web statistics (first party cookies) do not require consent. This is already the case under Dutch law, however, for tracking cookies consent is required prior to the placement of these third party cookies. The same consent requirements, as under the GDPR, apply: consent must be given freely, specific and informed. The GDPR also contains a "no bundling" provision. This means that you cannot, for example, ask for consent to access the site and at the same request consent for services that are not directly necessary to provide that access. The question is whether the use of tracking cookies (= advertising revenue) is necessary to keep websites online. This discussion will continue in the coming months.

For companies that use device fingerprinting, the consent issue will also be relevant. Device fingerprinting is the collection of data transmitted by a device (for example phone or laptop) when using the internet through an internet browser.
This includes data such as the operating system, set fonts, IP address and screen size, which allows a device and the user to be recognized. This information may only be collected when it is necessary to connect to the website and the visitor is

clearly informed about the collection and the possibility to opt-out. This will create an additional challenge for service providers who use device fingerprinting.

Fines
The substantial fines that can be imposed under the GDPR are well known. Under the e-Privacy Regulation, the same fines can be imposed by the Data Protection Authority. Under the current proposed e-Privacy Regulation, the fine for the incorrect use of cookies and the deployment of other marketing channels is up to 10 million euros, or 2% of the total annual worldwide revenue of the preceding fiscal year. An amendment has already been filed to increase the fine to 20 million euros or 4% of the total annual worldwide revenue of the preceding fiscal year. We have to wait and see whether this proposal will make it into the final regulation.

For many organizations, there is a still a lot of work to do before the GDPR is properly implemented. And, a new challenge is coming up with the proposal of the e-Privacy Regulation.

"An important starting point with the GDPR is the concept of personal data. The GDPR is only applicable when personal data is processed. Personal data is data by which a natural person can, directly or indirectly, be identified."

Privacy seals, certifications & marks possibilities as a result of the GDPR

GDPR World Series

The General Data Protection Regulation ('GDPR') will bring the possibility for businesses to apply for data protection certificates, seals and marks. In this blog, we will discuss this innovative approach to privacy compliance procedures and their potential to increase your company's competitive advantage.

By Filipa Carmo Pedro (Deloitte NL) and Ria Halme (Deloitte FI)

An official "stamp-of-approval"

Data protection certification, seal and mark mechanisms for processing operations, unheard of in the legislation that preceded the GDPR, are voluntary in nature. These mechanisms were included by the legislator to aid controllers and processors in demonstrating that the processing of personal data they carry out is compliant with the GDPR and helps businesses to ensure that appropriate technical and organizational measures are effectively in place. Moreover, such measures might prove to be particularly useful for controllers and processors in third countries – certificates held by these parties, if coupled together with binding enforceable commitments to apply appropriate safeguards, can be used as a legitimate basis for cross-border transfers of data. Certificates, seals and marks can be attributed to a controller or processor for a maximum period of three years, and can be renewed provided the same requirements are met at the time of renewal.

The GDPR defines as certification bodies:

- The competent supervisory authority;
- An accredited (public or private) body; and
- The European Data Protection Board ('EDPB').

As for the accreditation of certificate bodies, it shall be valid for a maximum period of five years with the possibility of renewal, provided the criteria set out by the national accreditation body / supervisory authority / EDPB are met.

Where the European Data Protection Board approves this criteria, this may result in a common certification (i.e. European Data Protection Seal), which is consistent with the GDPR's incentive to a uniform approach.

Lastly, and although the GPPR encourages businesses adherence to these mechanisms, there is still no EU-level uniform version of the requirements for certification, nor are there requirements in place for the aforementioned certification bodies to grant such a seal. Thus a common European Data Protection Seal is yet to be developed.

Acquiring a certification, seal or a mark

The specific processes and entities accredited to provide a company with a certificate, seal or a mark are still under discussion, and no decisions were made yet on how these will work. However, the GDPR states that Member States and relevant EU-level authorities shall encourage the establishment of these mechanisms. Hence, it can be expected this development will be based on already existing best practices and approved methods, instead of being started from scratch.

Moreover, publications of official EU-level authorities and several Article 29 Working Party ('Art 29 WP') guidelines have provided input on the interpretation of the GDPR, including references to existing commonly acquired technical standards, such as the ISO. Thus the Art 29 WP's guideline on Data Protection Impact Assessment ('DPIA') refers directly to the ISO-standard 31000:2009 as something that has been taken into account when drafting the guidance. Similarly, the European Data Protection Board will have mandate to enforce a technical privacy-enhancing standard on their own initiative.

Hence, a careful estimation is that the currently existing approved mechanisms can be taken into consideration when developing these instruments, enabling business to build upon existing methods, provided they are made GDPR-compliant.

Pros and cons

Prior to embarking on the use of these instruments, it is essential that your organization considers its pros and cons. For smaller companies, the costs can be substantial, as the renewal period is three years. The instrument itself also doesn't guarantee GDPR compliance on its own - additional measures are needed, and resources required need to be planned accordingly. Also, how the market will react remains to be seen. Thus the concrete added-value for the company will only be known once these mechanisms are implemented.

However, taking into account that consumer expectation upon their privacy has been on the rise, an official indication of GDPR compliance, even of a voluntary nature, enhances consumer trust and competitive advantage. A company which is able to show they have reached a certain level of privacy protection will be an easier choice for consumers as well as for business partners.

In addition, this enables vendors to acquire new businesses in an easier manner as a controller will be more likely to engage with a certified GDPR compliant processor. At the same time, a controller's choice based on this premise helps to demonstrate all appropriate measures were taken prior to outsourcing the processing of the data. It will be interesting to see how this will play out when the GDPR becomes enforceable, especially if we think about the example of cloud service providers, which many times have unnegotiable service level agreements and thus might benefit from an indication that they are serious about protecting privacy.

Instruments for demonstrating compliance are here to stay, but should be carefully analyzed on a case-by-case basis. That said, if done right, they are an effective and straightforward solution to demonstrate compliance and generate new business opportunities.

GDPR Update: The future of international data transfers

How will international data transfers be impacted by the GDPR?

We are more connected than ever. For any organization operating on a global scale, the international transfer of data is an essential element of daily business operations. Organizations may, for example, store customer personal data in a cloud service hosted abroad or may store employee personal data at a subsidiary established in another country. How will the upcoming General Data Protection Regulation (GDPR) affect such international data transfers? Let us explain!

By Nathalie McNabb (Deloitte NL) & Soeren Klaebel Clemmensen (Deloitte DK)

Adequate and "non-adequate" countries
The GDPR essentially distinguishes between countries outside the European Economic Area (EEA) that are considered to ensure an adequate level of protection for personal data and "non-adequate" countries. A transfer to an "adequate" country is the simplest way to transfer personal data outside the EEA; these transfers are permitted and legal under the GDPR. A transfer to an adequate country does not require prior approval from a supervisory authority and organizations need not take any further action.

What's the catch though? Only the European Commission can decide on adequacy, this is not a self-assessment. The full list of adequate countries can be found on the Commission's website.

"Non-adequate" country? Appropriate safeguards!
In the absence of a Commission adequacy decision, international data transfers may only take place where organizations have taken appropriate safeguards for the protection of personal data. This is to ensure that the level of protection offered by the GDPR is not undermined. The GDPR lists a number of possible safeguards that can be taken. Below, we discuss the two best known safeguards for organizations operating on a global scale: Binding Corporate Rules and Model Standard Clauses.

Binding Corporate Rules
Binding Corporate Rules (BCRs) is a mechanism whereby an organization can set out its global policy on the international transfer of personal data within that corporate group. Whilst the concept of BCRs may not be new (they existed pre-GDPR as well), the GDPR is expected to offer greater legal certainty to organizations considering adopting them. This is partially due to the new statutory recognition of BCRs as an appropriate safeguard as well as the fact that they must meet specific content requirements. Organizations are now better equipped to understand what is expected of them and to understand the requirements for obtaining approval. BCRs are furthermore subject to a new streamlined approval process whereby the approval is coordinated by one Data Protection Authority (DPA) in Europe and must follow set deadlines. There is therefore no longer a need to obtain approval from multiple DPAs and the timeline for approval should be better streamlined.

The initial investment of gaining approval is however particularly costly (both in monetary terms as well as in time) but there may be great benefits for larger organizations. BCRs must, for example, ensure compliance through mechanisms such as data protection audits and must ensure data protection training for personnel with access to personal data. Such content requirements can help stimulate a privacy-aware culture within the organization and help move the organization towards GDPR compliance. Moreover, after having obtained approval, transfers made in accordance with the BCRs require no further approval thereby limiting the administrative burden.

Furthermore, it is important to note that BCRs offer no solution for the international transfer of personal data to third parties. BCRs merely cover intra-group transfers and should not be considered as an adequate safeguard for international transfers outside the corporate group. BCRs are better suited for organizations with a complex web of internal processing activities. Gaining approval is a complicated process requiring a significant investment and it may be difficult to translate the BCR provisions into practical requirements. This investment may not pay off in the long-run for smaller organizations and such organizations may be more interested in adopting Standard Model Clauses instead.

Standard Model Clauses

Standard Model Clauses are essentially contracts approved by the European Commission that can be adopted for the transfer of personal data outside the EEA. Model Clauses already exist today but the Commission is expected to draft a set of new clauses to follow GDPR standards. The GDPR also introduces the possibility for local DPAs to draft Model Clauses. Model Clauses are considered to provide appropriate safeguards and hence have been widely used.

Model Clauses are popular amongst SME's for simple structural data transfers but this mechanism may be interesting for both private companies of any size as well as public entities. Model Clauses simply require a signature from the organization sending the data (data exporter) and the organization receiving it (data importer) under the condition that the data importer can comply with the stipulated provisions in the agreement. Model Clauses are therefore not recommended for larger organizations with complex processing activities as this solution would impose a heavy administrative burden and little flexibility given that new processing activities would require new Model Clauses to be signed.

Recently, however, concerns have been raised as to whether the Model Clauses sufficiently protect personal data transferred outside Europe. Consequently, a number of questions concerning the validity of the Model Clauses have been referred to the Court of Justice of the European Union. Organizations that rely on Model Clauses should therefore pay careful attention as the playing field may change in the future. In this quickly changing environment, organizations should prepare for alternative solutions or be ready to adapt if needed. For the time being, Model Clauses are still considered a valid option and should not be disregarded!

The impact is positive

Whilst the rules on international data transfers may at first sight seem complicated and difficult to navigate, the impact of the GDPR is likely to be positive for organizations. The GDPR offers a suitable solution for various types of organizations. Large organizations with a complex web of processing activities are more likely to opt for BCRs given their additional legal certainty and global impact, whereas organizations with a more limited network of international transfers may choose to adopt Model Clauses.

BCRs and Model Clauses are certainly the main appropriate safeguards for international transfers but it is important to note that the GDPR also offers other solutions:

- An approved certification mechanism whereby GDPR compliance is demonstrated through certification, data protection seals and marks together with binding and enforceable commitments;
- An approved code of conduct that stipulates the international transfer of personal data together with binding and enforceable commitments on how to apply the code of conduct.
- "Ad-hoc contracts" approved by a competent Supervisory Authority;
- Derogations such as explicit consent, transfers on the basis of performance of a contract, necessary for legal claims or defenses etc.
  The derogations should be used narrowly and only in exceptional cases. Consent is a complicated legal basis (individuals can withdraw their consent at any time!) and should not be used for international data transfers that take place on a large and/or structural basis.

GDPR and the impact on cloud computing

The effect on agreements between enterprises and cloud service providers

How will cloud computing change by the GDPR? What are the general privacy challenges and the GDPR specific challenges to anticipate?

By Alex Tolsma (Deloitte NL)

Moving to the cloud
More and more enterprises are moving to the cloud. This can have big advantages for an enterprise: it also allows for a better optimization of IT resources because cloud solutions are almost unlimited scalability and have a great flexibility. All at a contained cost.

Typically a cloud service provider would qualify as a processor when your enterprise uses their services. The cloud service provider will process personal data, which are stored within their databases or servers, on your behalf: the controller. The cloud service provider cannot do anything with your data, unless you instruct them to do so and the data remain within your controllership.

With the use of cloud services, challenges for enterprises will arise. Some challenges are (1) general privacy challenges of cloud computing and then (2) more GDPR specific challenges. These challenges must be anticipated when using cloud services, and the discussion of these challenges will form the main part of this blog.

General privacy challenges of cloud computing
One of these challenges in cloud computing is connected to the sensitivity of the entrusted information. As an enterprise you can host almost any type of information in the cloud, including sensitive information, which increases the risk of uncontrolled distribution of this information to third parties (i.e. competitors). Third parties you do not want to give access to your information. If a cloud computing solution is chosen where data processing and/or storing premises are shared, the risk of information leakage is present.

Next to this, it can be a challenge for enterprises to determine the applicable law. With cloud computing the relation of data to a geographical location can be blurred. It is not always clear where data are stored. Therefore it can be difficult for an enterprise to determine applicable law. Within the EU, the physical location is a decisive factor to determine which privacy rules apply. However, in other jurisdictions other regulations may apply. This challenge becomes more difficult because of the volatility of data in the cloud. Data may be transferred from one location to the other regularly or may reside on multiple locations at a time. This makes it hard to determine applicable law, and watch data flows.

Another challenge lies in the externalization of privacy. Enterprises that make uses of cloud service providers expect that the privacy commitments they have made to their own customers and employees will continue to apply by the cloud service provider. If such a provider operates in many jurisdictions, the exercise of rights of data subjects may be subject to different conditions as well. Therefore it is advised to try negotiate a tailored contract with clauses incorporated about these privacy commitments, next to agreements about the controller and processor relationship.

GDPR specific challenges
Implementing retention effectively in the cloud. In general, under the GDPR personal data may not be stored longer then needed for the predefined purpose. Therefore, retention periods must be implemented and it must be able to delete data effectively when retention periods has expired: both for data locally stored and in the cloud. The difficulty here is that data can be stored on multiple locations, under multiple jurisdictions, by cloud service providers, and therefore there is the challenge to identify and manage multi-jurisdictional retention requirements. The deletion of data will also impose a challenge. To delete data completely, backups must be taken into consideration as well. Therefore, it is important to have a clear overview of how backups are secured and retention is managed by your cloud service providers.

Breaching response and coordination. Breach notification obligations and protocols must be included in data processing agreements with cloud providers. The contract must define a breach event and describe a procedure for the provider to notify your enterprise about any breaches without undue delay. Even if the cloud provider experiences a data breach that impacts multiple customers, the controller (you) should own external communications and manage the overall breach with their support. What controllers don't want is a breach making headlines before their provider notifies them of the breach and before the controller is able to notify local authorities.

Processing of personal data outside the European Economic Area (EEA). Because data can be stored within multiple location by cloud service providers, it might be possible that personal data are stored outside the EEA. For this processing, appropriate safeguards must be taken if no adequacy decision have been made about the country where the data resides. Controllers will need to define a multi-country cloud strategy to adhere to adequacy requirements as well as data localization laws.

Data portability for the controller. Controllers must be able to facilitate the right of data portability for data subjects. If the data of the controller is in the cloud, it must be possible for the controller to retrieve the data in a structured, commonly used and machine-readable format to provide to the data subject or another controller. It is important to make agreements about this with cloud providers that are engaged by your enterprise. Providers will need to provide the technical capability to ensure controllers can satisfy this data subject right.

Data ownership. As a controller you must maintain control and ownership of your own data. Therefore this must be spelled out in contract. Next to this, you must confirm that, according to the host-countries' laws, your company retains ownership of the transferred data.

Risk management. Cloud service providers must be subject of your third party risk management. To determine any risks that may arise when using a cloud service provider a Data Protection Impact Assessment (DPIA) and a security assessment can be performed. Next to this, the right to audit cloud providers must be incorporated in the agreements concluded with these providers. In order to perform a proper audit, a control framework with privacy and privacy by design control measures must be defined next to an appropriate audit plan.

Cloud architecture and privacy by design. As a controller, when engaging a cloud provider, you should understand the underlying technologies the cloud provider uses and the implication that these technologies could have on the security safeguards and protection of the personal data stored in the cloud. The architecture of a cloud provider's system should be monitored to address any changes in technology and recommended updates to the system.

Visibility regarding metadata and Data Minimization. If you, as a controller, are interested in entering into a Service Contract for cloud services you should obtain information regarding the types of metadata collected by the Cloud Provider. Consider what level of protection is afforded to metadata, the respective ownership rights, rights to opt out of collection or distribution of metadata, and intended uses of metadata.

Security of Privacy. As a controller you are not in control over the cloud provider's (IT) environment and you must rely upon (IT) controls that the provider has in place. Therefore, it is always necessary to assess to what extent the provider is able to comply with your IT Security requirements. This could be done via the third party risk management process. Next to this, you also must assess what kind of IT Security and privacy measures or certifications the provider has in place. Cloud providers can demonstrate compliance with security and Privacy by Design in several ways:

- With the results of a performed DPIA;
- By being ISO 27001 certified (information security management system);
- By being ISO 27018 certified (code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors).

Next steps

If your enterprise is using cloud service providers it is necessary to have a good overview of your data lineage. You want to know where the data are stored, how it can be transferred and what access possibilities you have to your own data. The location of your data is important to determine applicable law. You also want to check whether the security measures the cloud provider has taken are sufficient, an audit can be a good measure to do an assessment on these measures so you want to incorporate this right in your agreements.

GDPR & Brexit: Is there a need for an adequacy decision?

What are the consequences of Brexit in relation to data transfers?

Brexit potentially affects all personal data exchanges between the EEA and the UK. This has also been stipulated by the European Commission consumer directorate in a Notice to Stakeholders issued on 9 January 2018. In this notice the European Commission advised stakeholders that cross-border data flows between the EU and the UK will not automatically have adequate safeguards anymore. What does this mean for the GDPR?

By Pieter Lamens (Deloitte NL) & Evelyn Caesar (Deloitte UK)

Countdown has started

The General Data Protection Regulation (GDPR) will come into effect on the 25th May 2018, updating the European privacy landscape. One of the major GDPR topics is the international transfer of personal data. It is relatively simple to transfer personal data outside the EEA (European Economic Area) to "adequate" third countries; these transfers are permitted and legal under GDPR and do not require prior approval from a Supervisory Authority. But only a handful of countries outside the EU have been deemed "adequate" by the EU. Previously in our GDPR article series our colleagues further elaborated on how international data transfers will be impacted by the GDPR.

While the UK is currently part of the EU, it is considered adequate and data can be freely transferred in both directions (between the UK and other EEA Member States). Due to Brexit, the UK may soon be considered non-adequate, i.e. a 'third country' (by 23:00 UK time on 29 March 2019, unless a withdrawal agreement between the EU and the UK establishes another date). This will impact transfers of personal data between the UK and the remaining EEA Member States; as the UK will be subject to Article 45 of the GDPR, data transfers will only be permissible if the UK, as a country outside the EEA, complies with one of the following:

1. Transfers will be permissible if the UK is approved by the European Commission to hold an adequate level of data protection and formally accepted as an 'adequate' third country (discussed below);
2. Transfers can be made if the UK makes use of model contractual clauses (approved by the European Commission and/or the relevant Supervisory Authority);
3. Transfers can be made if the UK makes use of ad-hoc contractual clauses (approved by the relevant Supervisory Authority);
4. Transfers may be made on the basis of approved codes of conduct/approved certification mechanisms; or
5. Supervisory Authority agreed binding corporate rules (BCRs) may be used to transfer data to/from the UK, when dealing with transfers between organization within a corporate group.

Is everyone on track? Is the UK on track?

Regarding the implementation of GDPR at Member State level, the EU Justice Commissioner Vera Jourova recently said that member states are lagging behind, and in particular have not yet amended their local legislation; thus far only Austria and Germany have implemented local laws incorporating GDPR. This might cause some application issues for the overall functioning of GDPR across Europe.

The UK has produced draft legislation to revise the Data Protection Act (1998) in line with GDPR. The Data Protection Bill (2017) is currently going through the process within the UK Parliament to be legislated as an Act. This may assist the UK with an adequacy decision, as it demonstrates to a degree that the UK is on par with the GDPR.

What about Brexit?
In this blog we will elaborate on the UK's situation, and in particular how it can become an adequate country. If an adequacy decision is not established, the other main options are:

- Governmental level: to have a bilateral agreement similar to the EU-US Privacy Shield in place
- For organisations to implement standard contract clauses (model clauses) or binding corporate rules for intragroup data transfers

These two options require substantial additional effort; especially the second option which would add complexity and costs to data transfers for organisations. In this blog we will only focus on the adequacy decision.

Adequacy decision
When the UK becomes a 'third country' after Brexit, for purposes of legal certainty and as the strongest guarantee of the free flow of personal data, an adequacy decision may be considered the preferred approach.

If the European Commission adopts an adequacy decision in respect of the UK, this would ensure an all-encompassing and clear agreement permitting transfers of personal data from the EU to the UK. The European Commission has already adopted an adequacy decision for several countries under the 1995 Directive, and adequacy talks are ongoing with Japan and South Korea. Keep in mind that the adequacy decision procedure can only be initiated officially once the UK becomes a third country and the procedure on average takes 28 months and can be revoked at any time.

The adoption of an adequacy decision involves a proposal from the European Commission, an opinion of the European Data Protection Board, an approval from representatives of EU countries and the adoption of the decision by the European Commissioners.

Will the UK have an adequate level of data protection?
In general the Commission assesses whether a country outside the EU offers an adequate level of data protection. The UK's domestic law (general and sectoral), international commitments, existing and functioning of the Supervisory Authority (the Information Commissioner's Office, ICO) will all be scrutinized.
The UK government's view is that an 'adequacy decision' should be easy to achieve as the GDPR is being brought into UK local law and the UK has a longstanding tradition of protecting personal data as a former EU Member State. According to the government the UK's data protection framework will be fully aligned with the GDPR at the date of withdrawal from the EU. However there are some challenges:

- The main potential problem is the UK's Investigatory Powers Act 2016, which allows for broad interception, interference and communications acquisition powers so as to limit the rights of individuals; essentially this Act may contravene the human rights element which the GDPR is fundamentally based upon and unfairly detriment the freedoms of individuals
- Also the UK has said it will not incorporate the Charter of Fundamental Rights of the EU. Articles 7 and 8 of this Charter constitute fundamental privacy rights and data protection rights and are the basis for the GDPR

Role of the ICO
The role of the ICO regarding regulatory cooperation between the UK and the EU will be of high importance. The UK government wants to ensure the ICO stayinvolved in future EU regulatory dialogue to allow the ICO to continue to share its resources and expertise. Also it aims to retain the ICO seat on the European Data Protection Board (replacement of the WP29 following the 25th May 2018). On a more positive note, the ICO currently already plays an active and progressive role in the field of EU Data Protection Authorities.

Is GDPR still revenant for UK businesses after Brexit? The answer is easy: Yes. GDPR is relevant.

- The UK will still be a member of the European Union at the point when GDPR comes into force and this means that until Brexit, the UK will be subject to GDPR in its entirety.
- If the UK were to negotiate to join the European Economic Area (EEA), GDPR would continue to apply post-Brexit. This 'Norway model' involves the implementation of EU laws in order gain access to the EU market and would mean that the UK would remain bound by implement amongst others the GDPR (and e-Privacy Directive). However, it should be noted that the UK government's stated objectives for Brexit do not include EEA membership.
- If the UK does not join the EEA, GDPR will in any event continue to apply to all UK entities that do business in the EU. If a UK business wants to conduct business with EU organizations it is likely to be required by GDPR and EU trading partners to have implemented appropriate data protection safeguards that protect the interests of individuals as good as GDPR standards.
- As mentioned above, the UK is working on the implementation of a new Data Protection Act. The UK's Department for Digital, Culture Media & Sport emphasized that an unhindered flow of (personal) data is essential to the UK forging its own path as an ambitious trading partner. That is why the UK government will be seeking to ensure that data flows between the UK and the EU remain uninterrupted after the UK's exit from the EU. In practice this will mean that the new UK Data Protection Act aims to assist with the full implementation of GDPR.

What do you need to do?

- UK-based firms should review their existing information security and data protection frameworks to ensure they are geared up for the new sharpened local and European data protection regulatory landscape.
- UK-based firms should think about their EU-UK data transfers pragmatically and document them sufficiently, in case the UK is deemed as inadequate.
- It is also advisable for firms to review their contracts, as some contracts (particularly business to business) include a 'no transferring data outside of the EU' clause; further to this, privacy notices need to also be assessed and updated where necessary, to ensure they are transparent in informing the data subject that their personal data will be passed out of the EU.
- International organisations, especially UK organisations with an EU presence, need assess whether their current data transfer practices will continue to be justified under the GDPR considering the Brexit implications. To support stakeholders the European Commission launched a dedicated webpage for businesses and citizens and is offering financial support to Member States to develop training materials and projects that support data protection authorities' work with businesses Overall, organisations must prepare for Brexit. When it comes to privacy and data protection, organisations should map their personal data flows, review contracts and data protection policies and put in position the appropriate mechanism for transfers of personal data to/from the UK.

"We are more connected than ever. For any organization operating on a global scale, the international transfer of data is an essential element of daily business operations. How will the GDPR affect international data transfers?"

GDPR Top Ten: #10 - One stop shop

The impact of the one stop shop mechanism

Supervisory authorities under the GDPR are tasked to enforce and provide guidance on privacy laws in a consistent manner across the EU. This article highlights how the one stop shop mechanism will facilitate consistent privacy law guidance and enforcement, and what impact this may have on organisations and consumers.

By Annika Sponselee & Rodney Mhungu (Deloitte NL)

The one stop shop mechanism

For organisations active in multiple EU countries, the GDPR provides a central point of enforcement through a system of co-operation and consistency procedures that has been coined the 'one stop shop' mechanism. This means that if your organisation conducts cross-border data processing, the GDPR will require you to work primarily with the supervisory authority based in the same Member State as your main establishment (usually your EU headquarters) to achieve compliance. This enforcement body will be your 'lead supervisory authority' for all privacy related matters.

In circumstances where individual data subjects of another Member State are substantially affected by your personal data processing activities, the local supervisory authority of that Member State may either hand the case over to your lead supervisory authority or handle the case locally in co-operation with your lead supervisory authority, depending on the most appropriate course of action for a legal remedy to a complainant. Notwithstanding these co-operation and consistency procedures, each supervisory authority in the EU will be competent to handle local complaints or infringements of the GDPR.

Essentially the one-stop shop mechanism intends to ensure that organisations and individuals can deal with cross-border privacy-related issues from their home-base, and that such issues can be addressed consistently across the EU.

The impact of the one stop shop mechanism on consumers

In line with GDPR's primary goal to protect consumers more effectively, the one stop shop mechanism is one of the many features of the GDPR that aims to make it easier for data subjects to exercise rights related to their personal data.

Data subjects can request information from their local supervisory authority about the exercise of their rights under the GDPR, which includes requests related to the cross-border processing by multinational organisations. The local supervisory authority is tasked to investigate local complaints and inform the complainant of the progress and outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary. In this respect, a consumer (data subject) can rely on their local supervisory authority to help protect their rights under the GDPR, no matter where an implicated organisation's EU headquarters are.

In effect, the current privacy regime already facilitates handling local complaints in this manner, so perhaps the GDPR complaint process may not affect the consumer's perspective on how they can exercise their rights. Consumers need to submit their complaints to the local authority today, they will need to do the same under the GDPR. Thus the biggest impact the one stop shop mechanism will have on consumers will likely be that complaints will be handled more efficiently than they are today.

The impact of the one stop shop mechanism on your organisation

There will likely remain a large administrative burden in coordinating cases involving cross-border data processing, but the lion's share of that burden will shift to regulators and away from controllers and processors of personal data. Under the current regime, the cooperation of data protection authorities (the functional equivalent of supervisory authorities under the GDPR) is strongly encouraged by policy makers, but no clear procedures are provided for in EU law. So if a multinational organisation needs to address privacy compliance in multiple countries, the organisation needs to become familiar with and address differing procedures in different Member States. However, when the GDRP is fully implemented on 25 May 2018, it will formally require supervisory authorities to co-operate with each other to align their guidance and enforcement procedures. This should mean that, by 2018, organisations operating across EU countries can mainly rely on the guidance and enforcement procedures of their lead supervisory authority, rather than engage with the procedures of many EU supervisory authorities.

Provided that you develop a compelling strategy for processing personal data, the promise of interacting with one clear voice of authority in EU privacy law should allow your strategy to produce its intended effects at a greater scale. This is because, on the one hand, the privacy strategy you devise based on the risks you have determined at your headquarters can be implemented consistently in every office; and on the other hand, your entire organisation can learn from the data processing experiences of each local office by feeding those experiences back to your organisation's center of gravity.

Leverage your lead supervisory authority to scale your privacy strategy

In sum, when the GDPR is fully implemented, the one stop shop mechanism should help consumers to exercise their rights related to their personal data more effeciently, and it should also become easier for your organisation to understand those rights and your privacy risks at an EU level.

You should thus make a focused effort to leverage the one stop shop mechanism and the guidance of your lead supervisory authority in order to simplify GDPR compliance. Your organisation will be able to consult closely with your lead supervisory authority in order to create a privacy strategy based on one clear set of privacy risks, implement that strategy across all of your (EU) offices, and learn from the local experiences of each office in order to consistently measure and improve the impact of your privacy strategy throughout your organisation

GDPR Top Ten: #9 - Security and breach notification

What does the GDPR say about how you should secure personal data?

Making sure that personal data is processed securely is an important aspect of privacy. And as security measure can take up two-thirds of your efforts when dealing with privacy, you also want to be efficient. So what does the new General Data Protection Regulation (GDPR) say about security?

By Jan-Jan Lowijs (Deloitte NL)

Modern security thinking

Once upon a time, security meant that you had a firewall to keep the bad guys out, and that every user had a password of no less than six characters to make sure their accounts could not be compromised. Those days are long gone. We now know from modern security thinking that taking only preventive measures (like firewalls and passwords) are no longer enough nor efficient. Security these days means you are able to prevent your digital assets from being compromised, but also able to detect when something threatens them and able to respond to incidents to bring the situation back to normal.

Now in the General Data Protection Regulation (GDPR) the security section has been much extended when compared to its predecessor, the Data Protection Directive. Security is now described in three articles (art. 32, 33 & 34), instead of one (art. 17), and it has been extended with breach notification obligations. Taking a closer look at Chapter IV, Section 2 of the GDPR, what does it actually say?

Secure the data you process

Under the regime of the GDPR you still have to make sure that you properly secure the personal data you process. The basic description of how to do so is unchanged compared to the definition in the Directive. Security is again described as a risk management process: you should first assess the risk, then look at what is possible in terms of security, and after having balanced risk versus costs, define your security measures.

Nothing new there, and by the way: proper information security has always been that way.

There are however some aspects to take into account.

- First, there is the notion that you should asses the risks for the rights and freedoms of natural persons, and not, say, the financial risks your organisation might face when the security of personal data gets compromised. You can of course include the latter, but including the former is a must. Security risk assessments regarding personal data should at least consider the impact of security failures on the individual – all the rest is optional.
- Second, the GDPR gives a number of examples of security measures. Pseudonymisation[1] and encryption of personal data are suggested as good security measures, as is the fact that security is about the Confidentiality – Integrity – Availability-triad and about being resilient to disruptions. Further, disaster recovery and having processes in place to regularly assess the state of your security measures are also suggestions given.
- Third, security is no longer the responsibility of the controller alone. The processor is addressed as well in the security articles of the GDPR. The processor now has an obligation to apply proper security measures independent of the controller. This also means processors can be addressed directly by the supervisory authorities when their security fails and are no longer shielded by the controllers.

[1] The GDPR defines pseudonymisation as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information."

Breach notification

New in the GDPR is the notion of breach notification: in case (preventive) security measures are breached and personal data is unlawfully processed, the controller must report such a breach to the supervisory authority within 72 hours, and possibly to affected data subjects as well. This is the case unless you can establish that the breach has caused no actual risks for the data subjects or other individuals.

Although new in the GDPR, this breach notification requirement is a well-known mechanism. It has been part of the ePrivacy Directive for some time now, meaning that telecommunications companies in the EU already deal with this on a daily basis. Also, a number of countries, the Netherlands among them, currently have breach notification obligations. As a result, numerous guidelines have already been published on how to establish whether a breach is severe enough to require notification, and if so, how breaches should be notified.

Having said all this, in case you do suffer a security breach (and it is not a question of whether it will happen to you, but when), breach notification should not be at the top of your mind. Responding to the breach should be, taking into account all actions that need taken care of: fighting possible intruders, establishing extent of the damage and restoring the situation back to normal. Notifying the breach to the supervisory authority is one of the elements of your response, but probably not your first.

To make sure that breach notification is properly executed, it should be firmly embedded within and throughout the whole of your security incident response plans. And, as with all other response processes, for breach notification a sub-process should be defined, including roles and responsibilities, process description, checklists, etc. This has the added advantage that, when security response plans are practiced (you do practice, don't you?), breach notification is automatically taken into account, as it should be.

Outlook

What does this all mean? Should you now encrypt and pseudonymise every little snippet of data you processes? Should you redefine your entire incident handling processes making it revolve around breach notifications? No, that would be the wrong reaction.

You should resist those urges and keep acting like you always did (or should have done): make sure you perform proper risk assessments and then define your security measures based on these assessments. Address technical and organisational security measures and importantly, measures in all three areas of prevent, detect and respond. Lastly, part of your response measures should include the breach notification processes.

In the end, if you already run an effective and efficient security organisation, the GDPR tells you to keep up the good work. If you are not quite on that level yet, the GDPR encourages you to get up there. All with the end goal in mind: if you want to be trusted with other people's personal data, make sure you deserve that trust by properly securing it.

GDPR Top Ten: #8 - Pseudonymization and its use in profiling

How pseudonymization can benefit you and your customers

This blog focuses on pseudonymization: what is pseudonymization and how is it different from - the better known - anonymization? How can you use pseudonymization when you perform profiling and how can you use it on your data? How can pseudonymization be of added value to both your organization and your customers?

By Nicole Vreeman (Deloitte NL)

The word pseudonymization occurs in some form 15 times in the General Data Protection Regulation (GDPR) that will come into force on 25 May 2018. It does not occur in the Directive, the current EU privacy legislation. Similarly, the word "profiling" does not occur in the Directive, yet occurs 23 times in the GDPR. Why this change?

The Article 29 Working Party has already mentioned the concepts of pseudonymization and profiling in multiple opinions and publications that it has issued throughout the years. The concept of pseudonymization and the use of profiling are not new. You have most likely heard of them. Moreover, the concept of profiling was included and restricted in the Directive, but it was referred to as "automated decision-making".

What is pseudonymization and what is profiling?
Pseudonymization uses a form of encryption to translate identifiable parts of personal data to unique artificial identifiers, so-called pseudonyms. It aims to decouple the "personal" in personal data. This makes the data 'anonymous' within a limited context. Outside of this context the person can still be re-identified. By using pseudonymization you are applying a security measure to the personal data you have in order to prevent linking that data to the original identity of a person.

Pseudonymized data can still be traced to the data subject. You may need external information to do so, but all pieces of the puzzle still exist, just not all in one place. With anonymized data on the other hand, the original source data is deleted and therefore inaccessible and irreproducible.

Profiling according to the GDPR means "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person".

Profiling can also be used for predicting the data subject's behavior and can be a valuable direct or indirect marketing tool. Note that the GDPR provides that data subjects shall not to be subject to decisions based solely on automated processing (including profiling) when this processing has legal or similarly significant consequences for them. For example, it is prohibited to deny a request for a loan solely based on the automated processing of the information about the individual, since this results in significant (and potentially legal) consequences for that person. The right to object afforded to data subjects by the GDPR explicitly mentions profiling.

How your company or organization can use pseudonymization to its advantage
Pseudonymized data is suitable for a great range of analytical activities, research projects and for statistical purposes. Because not all personal data is exposed, it decreases the risk of abuse of the exposed data in the case of a data breach. The GDPR sets more relaxed standards for data that is pseudonymized as compared to personal data and seems to be nudging companies and organizations to use pseudonymization as a method of securing the personal data they process. Moreover, when data is pseudonymized it is less like to "significantly affect" the data subject or produce "legal effects" for the data subject, because the data subject can be identified less easily.

If you apply profiling in your organization, pseudonomyzing the data used in the profiling will be subject to the more relaxed standards mentioned earlier. Pseudonymizing the data may provide a "suitable measure" to safeguard data subjects' rights, freedoms and legitimate interests. Profiling may also have positive effects for your clients: based on the information your clients have provided and your profiling exercise, you may be able to offer an identifiable group of clients products aimed specifically at that group.

When done right, application of pseudonymization can offer more data processing possibilities, including profiling, than if the data were to be processed without applying pseudonymization as a security measure. You need to keep in mind, however, that it does not render the data anonymous. Pseudonymized data is still considered to be personal data and you need to treat it as such. Even if you have pseudonymized data, in case of a data leak, you may still be obliged to inform the affected data subjects.

"The GDPR sets more relaxed standards for data that is pseudonymized as compared to personal data and seems to be nudging companies and organizations to use pseudonymization as a method of securing the personal data they process."

GDPR Top Ten: #7 - Data Protection Authority enforcement methods

What enforcement methods are at the disposal of the DPA to ensure compliance?

The new GDPR will introduce new data subject rights and rules governing those rights. Rights and rules that are useless if compliance cannot be enforced. What enforcement methods are at the disposal of the DPA to ensure enforcement?

By Alex Tolsma (Deloitte NL)

From May 2018 the European Union will have a new, EU-wide applicable, privacy law: The General Data Protection Regulation (GDPR). This new regulation shall have equal legal force throughout the EU.
The GDPR will not only bring several new data subject rights, but it will also introduce a variety of new rules to which companies and individuals must adhere and be able to demonstrate compliance.
What are these rules? What are the ramifications of not complying with these rules? How will this impact your organization (e.g. financially, strategically, etc.)? And most importantly, how will compliance be enforced?

New data subject rights under the GDPR includes - among others - the right of data portability, the right to restrict processing, and the right to be informed of the right to object to processing by the controllers.

The GDPR sets out the obligation for Member States to set up a supervisory authority; the so called Data Protection Authorities (DPA). The task of these national authorities will be to monitor the application of the Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.
The obligation of the DPA from an enforcement perspective can then be divided into two parts:
1. Monitoring whether individuals can exercise their rights; and
2. Evaluating whether the processing of personal data complies with the rules on processing set out by the GDPR.

Suspicion of a violation
The DPA will have a variety of investigative powers to find out if a violation exists or not. To investigate a possible violation the DPA can order the controller and the processor to provide any information it requires for the performance of its tasks. The DPA may further request access to all personal data and to all information necessary for the performance of its tasks. An investigation itself may consist of data protection audits, and when necessary the DPA can obtain access to any premises of the controller and the processor, including to any data processing equipment and means. Where it is foreseeable that a manner of processing will not be compliant with the GDPR the DPA can issue warnings to a controller or processor.

Confirmed Violations
If the DPA concludes that a violation has taken place, there are several measures at its disposal. The least intrusive measure is the possibility to issue reprimands to a controller or a processor where processing operations have infringed provisions of the GDPR. If a reprimand is not sufficient, the DPA may also order the controller or processor to bring the processing operations into compliance with the provisions of the GDPR. If a controller or processor has ignored the rights of a data subject the DPA may order them to comply with the data subject's requests to exercise their rights. Moreover, the DPA can order the rectification or erasure of personal data or restriction of processing to meet the rights of data subject.
Data driven organizations or organizations that must process data as part of their business model can be severally impacted if forced to delete all their data due to compliance violations. Data for many organizations is seen more and more as the company's most valuable asset. In the case of a data breach the DPA can order the controller to communicate this personal data breach to the data subject.

If you apply profiling in your organization, pseudonomyzing the data used in the profiling will be subject to the more relaxed standards mentioned earlier. Pseudonymizing the data may provide a "suitable measure" to safeguard data subjects' rights, freedoms and legitimate interests. Profiling may also have positive effects for your clients: based on the information your clients have provided and your profiling exercise, you may be able to offer an identifiable group of clients products aimed specifically at that group.

When done right, application of pseudonymization can offer more data processing possibilities, including profiling, than if the data were to be processed without applying pseudonymization as a security measure. You need to keep in mind, however, that it does not render the data anonymous. Pseudonymized data is still considered to be personal data and you need to treat it as such. Even if you have pseudonymized data, in case of a data leak, you may still be obliged to inform the affected data subjects.

Severe Measure

If severe measures are necessary, for example because it appears that less serious measures have not led to the desired result, such measures are also at the disposal of the DPA. In that case the DPA will have the power to impose a temporary or definitive limitation including a ban on processing. This can have a significant impact on an organization's business operations, ability to service its customers and meet its overall business objectives. The DPA may also order the revocation of a certification (which is used to indicate that processing takes place in accordance with the GDPR). Moreover, the DPA may order the suspension of data flows to a recipient in a third country or to an international organization if applicable.

Levying of Fines

The most far-reaching powers consist of the imposition of administrative fines. If there is a less serious violation the administrative fines can go up to 10 000 000 EUR (10 million euro), or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. In case of more serious violations this goes up to 20 000 000 EUR (20 million euro) or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. These fines are substantial and can financially cripple companies and even put some companies out of business. It is therefore important to fulfill the obligations under the GDPR.

GDPR Top Ten: #6: Privacy by Design and by default

A good idea formalized

The General Data Protection Regulation (GDPR) changes European privacy rules significantly. The introduction of the concepts 'Privacy by Design' and 'Privacy by Default' are two of these changes. Although new as a legal requirement under the GDPR, these concepts are not new. Considering privacy from the start of the development process is essential to address privacy successfully.

By Shay Danon (Deloitte NL)

Essential part to the GDPR

The GDPR changes European privacy rules significantly. The introduction of the concepts 'Privacy by Design' and 'Privacy by Default' are two of these changes. Privacy by Designs holds that organizations need to consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data. Privacy by default means that when a system or service includes choices for the individual on how much personal data he/she shares with others, the default settings should be the most privacy friendly ones. Although Privacy by Design and Privacy by Default will become new legal requirements under the GDPR, these concepts are not new. Considering privacy from the start of the development process is essential to address privacy successfully.

Increasing efficiency by thinking of privacy in advance

Under the current Directive, data controllers already need to implement appropriate technical and organizational measures to protect data against unlawful processing. This, however, leaves room for privacy considerations to be reduced to a mere afterthought in the development process. The GDPR requires organizations to consider privacy at the earliest stage. Privacy must be one of the ingredients of a new product or service, rather than a sauce that is added at the end. This might seem complex, but it is actually easier than applying privacy considerations after a design is fully developed. When you think upfront about what personal data you want to use, for what purpose and how you will do this legitimately, it reduces the chance that you discover at a later stage that embedding privacy is technologically challenging, expensive or even impossible.

The application of Privacy by Design will therefore make the development process more efficient. Knowing what data you want to use, and giving data subjects a choice on how their data is used by applying Privacy by Default, will also make it easier to be transparent those data subjects. And transparency is key when it comes to earning the trust to collect the data in the first place. In other words: applying Privacy by Design and Privacy by Default is simply a good idea. That is why many organizations already have incorporated these concepts in to their development processes.

Embedding privacy in the design process, where to start?

In order to embed privacy in the design process several aspects must be taken into consideration.

- Operate within legal boundaries and be accountable
  Under the GDPR organizations will not only be responsible for adhering to privacy principles, they must be able to demonstrate compliance with them too. A privacy strategy is essential to make choices early in the development process regarding how you want to deal with privacy within your new service or product. Assess upfront if the idea can be executed within the relevant legal boundaries. A good instrument for doing this is carrying out a Privacy Impact Assessment (PIA). A PIA will help you identify privacy risks within your new design. Don't forget to keep your PIA findings. This will allow you to demonstrate your rationale behind certain decisions at a later stage.
- Think of ethics
  The ethical aspects of the concept must also be taken into consideration early on. An organization should determine how transparent it wants to be on its data processing and how much it wants to know about data subjects involved. A helpful questions is: would you use the product or service yourself?

- Communication is key
  Communication towards data subjects is very important to address at the initial design stages and throughout the complete development process. Communication lines must be clear, also when something goes wrong. For data subjects it must be clear where they can turn if they want to know more about the processing of their personal data and how they can exercise their rights.
- Data security, quality and retirement
  And of course it is important to think about adequate security measures, how the quality of data can be guaranteed and what will be done with the data when the product or service retires.

Implementation

Successful implementation of both Privacy by Design and Privacy by Default requires that employees - especially those involved in the development of new products and services - have enough basic knowledge on privacy. Clear policies, guidelines and work instructions related to data protection should be developed and a privacy specialist should be available to assist in applying these requirements. The development method (agile, waterfall etc.) used within the organization must be taken into account, in order to apply the concepts throughout the whole development process. This will enable the development teams to take appropriate measures in the relevant phases. And finally, when a design has been completed, it must be adopted by the organization and monitored throughout its lifetime.

Privacy by Design and by Default, what is not to like?

Mandating Privacy by Design and by Default is the formalization of a good idea. The GDPR aims to give data subjects more power over their personal data. Implementing Privacy by Design and Privacy by Default clearly reflects that aim. Offering the most privacy friendly option as a default setting will give people an actual say over which parts of their personal data can be used. The incorporation of Privacy by Design in the development process is the only way to apply privacy successfully. For organizations these concepts provide an opportunity to increase efficiency and gain data subjects' trust. What is there not to like?

GDPR Top Ten: #5 – New Data Subject Rights

The GDPR imposes new requirements for your organization regarding data subject rights. What are these requirements and how can your organization respond?

The General Data Protection Regulation (GDPR) changes European privacy rules significantly. The introduction of the concepts 'Privacy by Design' and 'Privacy by Default' are two of these changes. Although new as a legal requirement under the GDPR, these concepts are not new. Considering privacy from the start of the development process is essential to address privacy successfully.

By Sebastian le Cat (Deloitte AUS)

New perspective on existing rights

The General Data Protection Regulation (GDPR) will replace the current Data Protection Directive (95/46/EC) in 2018 and incorporate new rights and protections for data subjects. Rights such as the right to be forgotten and the right to data portability bring a new perspective on existing rights and may include new obligations for your organization. This blog explains how the new requirements may affect your organization.

The right to access, rectification, objection, restriction and notice

Before you can start processing personal data, you should provide information to the individuals whose information you will be processing. Under the GDPR, it should be possible for individuals to access their personal data upon request. Furthermore, the purpose of processing, categories of personal data, recipients of the data and a copy of the collected personal data should be available. When data about an individual is inaccurate or incomplete, individuals have the right to request a rectification. If the incorrect data is transmitted to third parties, your organization is also required to inform these parties about the incorrect data, unless this requires a disproportionate effort. Your organization is required to respond to all requests within one month, which could be extended by two additional months depending on the complexity of the request. Data subjects also have the right to object. If a person objects to data processing activities, your organization has to end such activities. If you really need to continue processing, you must be able to prove that you have compelling legitimate grounds that override the interests, rights and freedoms of the data subject.

The right to be forgotten

The right to be forgotten (in the GDPR also described as the right to erasure) has been talked about a lot, and there have been many misunderstandings about its application. It requires your organization to erase the personal data of a person within one month if:

- Personal data are no longer necessary for the initial purpose
- The data subject withdraws consent
- The data subject objects to the processing
- Data is unlawfully processed

If one or more of these grounds apply you must take reasonable steps to erase the personal data. This includes requesting third parties to remove such data as well. If your organization has made the personal data public, you should also inform other parties who process the personal data. However, the right to be forgotten is not absolute. A request for deletion can be denied, for instance in case the right of freedom of expression and information prevails or if the processing is in the public interest.

The right to data portability

New in the GDPR is the right to data portability. The right to data portability creates the possibility for data subjects to obtain and reuse their personal data across different services. The data subject is entitled to request a copy of their data in a structured, commonly used and machine-readable format. The data subject can then transmit their data to another controller of their choice.

The implementation of data portability in your organization can be divided into different stages. First of all you need to adjust your systems to facilitate a data portability request. The system must be able to provide the option to access, erase, restrict and adjust the data.

Secondly, you need to implement a structured process to fulfil the request smoothly. To respond within the given timeframe, it is important to communicate between different departments such as Legal, IT and Communication.

Data portability is not an absolute right, and a determination must be made with regard to legitimacy of the request: it should for instance be weighed against the rights of others. The processing must also be based on the user's consent or a contract, otherwise the right to data portability does not apply and your organization is not required to fulfil the request.

The new right to data portability imposes fairly invasive obligations for your organization. If you are able to implement the right to data portability you will likely cover many data subject's rights in general. This also goes the other way: if you already have processes in place to fulfil erasure, access and restriction requests you may be just a few steps away of full compliance with the right to data portability.

GDPR Top Ten: #4 Maintaining records of processing activities

What is the impact of this (new) obligation under the GDPR?

In this blog we focus on the technical and operational aspects of how organizations can create an overview of existing data processing activities. For some countries this is not an entirely new requirement, as organizations in for example the Netherlands and Belgium are already familiar with the obligation of notifying processing activities to the local Data Protection Authority.

By Robyn Post (NL)

This new responsibility for organizations, laid down in article 30 of the GDPR, requires a full overview of the processing activities that take place within an organization, but also requires these activities to be documented accordingly. This will require a proactive approach from, and collaboration within, organizations.

What does this new obligation entail for controllers?
Each controller will have the responsibility to maintain records of all the processing activities which take place within the organization. These records (which need to be in writing, as well as in electronic form) must contain all of the following information:

a) the name and contact details of the controller and where applicable, the data protection office;
(b) the purposes of the processing;
(c) a description of the categories of data subjects and of the categories of personal data;
(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;
(e) the transfers of personal data to a third country or an international organization, including the documentation of suitable safeguards;
(f) the envisaged time limits for erasure of the different categories of data; and
(g) a general description of the applied technical and organizational security measures.

Please note that the obligation does not apply to organizations employing fewer than 250 persons, unless the processing is of a high-risk nature, including processing of special categories of personal data such as ethnic or health information, or data about criminal behavior.

Furthermore, the controller or the processor (please refer to the next paragraph) need to make the records available to the supervisory authority upon request.

And what about processors?
In general, the GDPR does not only require more responsibility from the controller, but it also requires more responsibility from the involved data processors. Therefore, this obligation is also applicable to processors. Each processor will have the responsibility to maintain records of all categories of processing activities carried out on behalf of a controller, containing:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable and the data protection officer;
- the categories of processing carried out on behalf of each controller;
- transfers of personal data to a third country or an international organization, including the documentation of suitable safeguards;
- a general description of the applied technical and organizational security measures.

Operational and technical measures
Organizing records of all the data processing activities that take place within in your organization, could pose a challenge. Especially when these kinds of processing activities take place decentralized within different departments or business units. How can this stream of information best be coordinated, where should records be stored and more importantly, how should these records be maintained and kept up-to-date? Below a few practical tips and tricks are outlined.

1. Involve the business
As data processing activities take place across your organization, it is key to localize the stakeholders which play a role at the beginning of the development or design of a product, process, system, application or project. These people have the main insight into the data processing activities and will be of extreme value to create and maintain the overview. Involve the business when your organization starts to think about the underlying process that is needed to generate these records. Make them aware of the benefits and the added value for your organization.

2. Design (and align) a process, with clear roles and responsibilities
When you have your stakeholders involved, the next step is to determine the process in which the records must be obtained, checked, added to a central register and kept up-to-date. Be aware that lot of the required information will most probably already be obtained by performing Privacy Impact Assessments (PIA's). If there is an existing supporting process, explore to what extent this new process can be aligned. This will coordinate the required effort, and will prevent the business from providing the required information twice.

Also, make sure that clear roles and responsibilities are defined when the process is being developed. Think about responsibilities with regard to the collection of the required information, including the information into a centralized register and updating the information in the register when needed.

Do not forget to involve other competences as well, such as IT, compliance, procurement and legal, as they could also greatly benefit from the information. Think of the contracts in light of the procurement process in case processors are (going to be) involved. The information will be of great value in settling data processing agreements.

3. Create a central register for the records.
The records that must be kept, should be stored in a centralized manner. Depending on the infrastructure of the specific organization, explore how to support the fundamental process. Preferably, organizations should not "seek refuge" in Excel sheets, as easy as it might be – but rather use a proper tool. In this way one centralized system will provide a full overview of the processing activities that take place within the organization. Of course in this scenario people have to be aware of the proper technical measures, such as access and authorization rights (not everyone should be authorized to change or alter information). The market for privacy tools is expanding rapidly, and it is good to think about the technical requirements and possibilities within your own organization.

Is this obligation a burden or could it become a valuable asset for organizations?
This requirement under the GDPR will require some extensive effort. The organizing part will require a lot of the business, but also of the privacy professionals involved. To convince the business of the added value of these records – besides the fact that it is an obligation of which non-compliance could lead to fines up to EUR 10.000.000 or 2% of the total worldwide annual turnover – will take time. Keeping in mind the development of the process, but also exploring and implementing the technical measures, it will be a time consuming process. Moreover, don't forget

to keep track of existing processing activities: not only new data processing activities must be recorded, but also the activities that are taking place at the moment (and maybe have been for years).

However, there is also something to gain. The records will provide an overview of all data processing activities within your organization, and therefore enable organizations to get a grip on what kind of data categories are being processed, by whom (which departments or business units) and for which underlying purposes. This knowledge will allow organizations to make connections internally, join efforts or projects with the same or equivalent goals and / or challenges and it can result in increasing control over data processing activities. This will provide insight into risks and required mitigation actions, and will inevitably result in empowering organizations to do more – and in a well-ordered manner – with the available personal data.

GDPR Top Ten: #3 Extraterritorial applicability of the GDPR

Explaining the territorial scope of the GDPR and the situations in which its obligations apply outside the European Union

With the introduction of the GDPR, European data protection law will become applicable outside the borders of the European Union. In this blog we will give you an overview of the situations in which a non-EU organisation could fall within the scope of the GDPR when targeting or monitoring individuals in Europe.

By Alexander Garrelfs (Deloitte NL)

A peculiar environment
The internet is a space where none of the conventional borders exist. This is one of its biggest advantages when you exchange data, buy or sell online, communicate, etc. It also presents one of its biggest challenges when it comes to the applicability of legislation. Because of this borderless characteristic of the internet, for a long time the question was how to deal with EU privacy rules when processing personal data in connection with online services.

Before the introduction of the GDPR it was hard to apply the obligations of privacy legislation to data controllers and processors outside the EU. The main reason for this was the lack of focus on the individuals whose data was being processed when the applicability of the legislation was determined. The only way to make privacy legislation applicable to a controller outside the EU was if the processing by that controller was performed within the borders of the EU. However the GDPR brings rigorous changes to that concept of territorial scope.

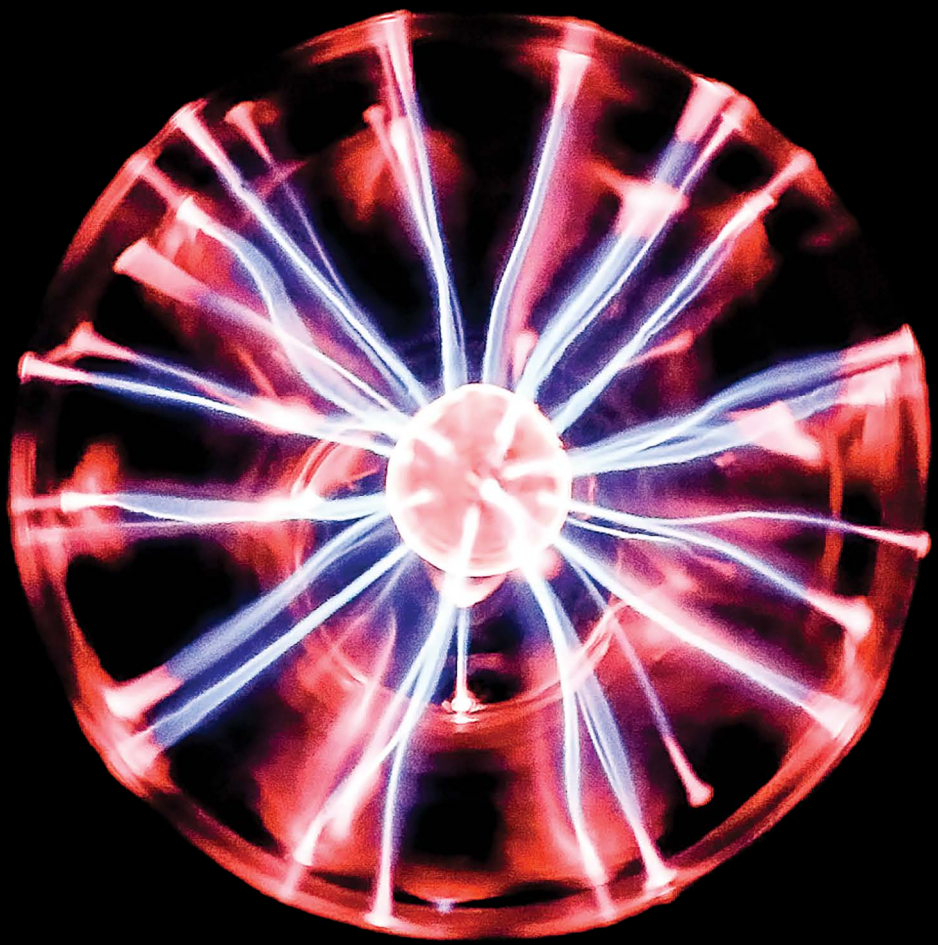
Scoping the territorial scope
Any organization – bar a few exceptions – that processes personal data within the European Union will fall under the scope of the GDPR. Nothing has changed here when compared to the pre-GDPR situation. However, the territorial scope has been broadened so that the EU privacy rules now also can apply to data controllers outside the EU. The consequence of this expansion is that under the GDPR non-EU data controllers and processors must comply with the European Data Protection obligations when they process data from individuals in the EU for specific goals.

Targeting EU citizens
As a non-EU organisation you can fall in the scope of the GDPR when you are offering goods or services to individuals in the EU. Let's say for example that you are a Chinese web shop with a website that is available in German, French and English as well. You also process multiple orders a day from individuals within the EU and ship your products to them. This will make you fall in the scope of the GDPR, even though you have no establishment in the EU and are not performing any data processing activities within the EU.

If you are a controller outside of the EU, such as in the example above, it doesn't matter if the services that you offer are paid or for free, the GDPR does not consider this aspect to determine if you fall within the scope. As such an American free cloud storage service must comply with all the obligations of the GDPR if the service is also offered to users within the EU.

Monitoring EU-citizens
Another situation in which non-EU organisations can fall within the scope of the GDPR is when they are monitoring the behavior of individuals inside the Union. This means that if you are a provider of social networks and you allow users from within the EU to join, that you fall within the scope of GDPR. The same goes for an app developer that decides to gather location data of EU citizens from their smartphones.

What's your approach?
The GDPR will offer a high level of protection to individuals in the EU whose data is processed by organisations that are established outside the Union. For companies it's important to evaluate if these new obligations will be applicable to them. If this is the case, taking action and making sure you are compliant will be the best course of action. You'll have to make your own bed, so be sure to lie comfortably!



GDPR Top Ten: #2 Accountability principle

What do organisations need to do to show accountability for their data processing activities?

The principle of accountability aims to guarantee compliance with the Data Protection Principles. It implies a cultural change which endorses transparent data protection, privacy policies & user control, internal clarity and procedures for operationalising privacy and high level demonstrable responsibility to external stakeholders & Data Protection Authorities.

By Sebastian le Cat (Deloitte AUS)

The principle of accountability

The General Data Protection Regulation (GDPR) introduces a new principle to data protection rules in Europe: that of accountability. The GDPR requires that the controller is responsible for making sure all privacy principles are adhered to. Moreover, the GDPR requires that your organisation can demonstrate compliance with all the principles. So, which steps should your organisation take to build such a culture and to be able to demonstrate accountability?

Firstly, the organisation must know what principles need to be adhered to. There are six principles set out in the GDPR. These are the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity and confidentiality. One of the best ways to make sure these principles are adhered to is to make sure your internal privacy governance structure is set up correctly and comprehensively.

The ways to incorporate these principles are woven in throughout the GDPR. For instance, the GDPR states your organisation is required to deploy appropriate technical and organisational measures as laid out in the GDPR. Some (new) measures mentioned in the GDPR are: documented processes/policies, data protection impact assessments (DPIA), suggested data security methods, data protection by design and by default, a mandatory data protection officer (DPO) for large scale personal data processing, and keeping records of your processing activities. Special attention is given to (industry) code of conducts and self-certification, data breach notification and transparency requirements.

A culture and organisational change

A strong governance structure is essential to standardise privacy and develop privacy by design and default. To create a cultural and organisational change for GDPR compliance within your organisation, buy-in from stakeholders is of significant importance. By developing internal guidelines for employees, compliance with legal obligations for data processing and securing data can be ensured. Incorporate training and awareness programs for everyone who is going to be involved in the processing of personal data. Your organisation can also consider subscribing to an industry code of conduct or creating internal guidelines and a review process for data analytics.

Subscribing to an industry code of conduct can demonstrate compliance, especially when the certifications are issued by the certification bodies. These mechanisms are not obligatory under the GDPR, but are highly recommended. Developing your own ethical standards with respect to processing personal data, may further enhance your accountability efforts. The risks of new initiatives are weighed against possible benefits. Questions like 'can we legally do this?' should be complemented by 'do we want to do this and how will it be perceived by our customers?' to safeguard the ethical use of the data.

Furthermore the GDPR obligates your organisation to maintain an internal record of all your processing activities. Your organisation is, among others things, required to record the purposes of the processing and a description of technical and organisational security measures.

New in the GDPR is the requirement to designate a Data Privacy Officer (DPO) within your organisation. Although the requirement is only mandatory in certain circumstances, a DPO can monitor the activities of your organisation and the processing activities to help you become compliant with the GDPR.

Conclusion

Under the GDPR, the principle of accountability becomes more important. Your organisation is not only required to adhere to the principles set out in the GDPR, but must also demonstrate compliance. To live up to the principle of accountability a comprehensive governance structure is necessary. Adhering to the principle of accountability means a cultural and organisational shift in your organisation. With the help of strong technical and organisational measures your organisation can demonstrate compliance with the GDPR.

"To live up to the principle of accountability a comprehensive governance structure is necessary. Adhering to the principle of accountability means a cultural and organisational shift in your organisation."

GDPR Top Ten: #1 Data Portability

Legal obstacle or opportunity?

Data portability creates a new right for individuals to have more control over their own data. This new right could lead to considerable costs for organizations, but it also provides a strategic opportunity if implemented in the right manner.

By Michiel van Schaijck (Deloitte NL)

Introduction: GDPR obligation difficulties

According to the IAPP Annual Privacy Governance Report 2016 data controllers consider three aspects of the GDPR most challenging to implement in their organization: the right to be forgotten, data portability and gathering explicit consent. In this blog we will elaborate on why the implementation of the GDPR and the right of data portability deserves your attention and why this represents a risk but also a strategic opportunity for your organization.

What is data portability?

"Data Portability" is 1) the ability and capacity to export data collected or stored digitally concerning a data subject AND 2) the ability to receive data concerning the data subject and to allow another controller to receive portable data. The Data Portability requirement entails both a technical design requirement and a data subject rights requirement. From a technical perspective, data controllers will need to ensure their systems, connected products, applications and devices that collect and store information on data subject also have the added functionality of porting and transmitting data. In some cases, this will require controllers to tweak or redesign some systems, products, applications and devices. Furthermore, the new porting functionality must export data in a structured, commonly used and machine-readable format so that reuse of the data is possible.

From a data subject's right perspective, the right to data portability creates a new right for individuals to exercise more control over their own data. It enables individuals to receive personal data concerning him or her, which he or she has provided to a controller. Thus, data controllers will need to establish and implement processes, in addition to added systems and digital propositions/products functionality, that aid in processing data subject requests whether in manually or in automated fashion. After receiving the data the individual must be able to transmit this data to another controller without creating additional burden or hindrance to the previous data controller. The right to port data also entails that where technically feasible, the personal data will be transmitted directly from one controller to another. Please be aware that the right to request a copy in a machine readable format is only possible if the data concerned was i) provided by the individual to the controller; ii) processed by automated means, and iii) processed based on consent or fulfilment of a contract.

Linked to other rights

Data portability is part of a larger spectrum of data subject rights: access to and rectification or erasure of personal data, the right to object to decisions based on automated means, as well as notifying data subjects of a personal data breach. Again, data controllers will need to implement supporting processes to be able to comply with these requests. For a data controller the process to carry out a request to port data could imply that you must facilitate different actions that are similar to the execution of other data subject rights. First, you may have to give the individual access to the personal information so that he knows what personal data is being processed. Second, you could have to rectify inaccuracies if the individual requests so; and third you might have to erase all the personal data (compliant with established retention schedules and legal contracts) if the individual asks to transfer his data to another service provider. Therefore three other data subject rights could be impacted when processing a data portability related request. Note however that the right of access, rectification and erasure are not similar to the right to data portability, it merely could imply that the data controller uses the same processes for these rights as it would need to facilitate the right to data portability.

In practice
In practice this means that you have to have the ability to provide your client or customer with a copy of all the personal data that you have regarding him or her; and the ability to transfer the data to another data controller or service provider. The data that you have regarding a costumer or client is interpreted as all the data that the individual has provided actively and knowingly. This includes information the individual has provided to you by using the service or device (for example, location data or heartbeat from a fitness tracker). This could therefore be a large collection of data. Furthermore the data must be provided in a way that facilitates reuse. For example, email must be provided in a format which preserves all the meta-data to allow effective reuse. Providing emails in pdf format would not suffice, because this is insufficiently structured for reuse. To comply with a request for data portability could be time consuming and lead to considerable costs for many organizations that have not already adopted a privacy by design approach to the design and build of their systems and digital products and propositions.

Large impact
The reason why this right is expected to have a large impact on your business, is that it alters the relationship between individuals and data controllers. Individuals are enabled to manage their data across different platforms, via for example a direct download tool or application. Eventually the platform that the individual prefers shall receive all the personal data. If you are not the preferred platform you might be obligated to transfer your data to a competitor and potentially be requested to erase the (valuable) data you have collected over the years. This leads to more competition between data controllers and should be taken into account when determining your business strategy.

Make it an advantage
i) Try to be efficient. Controllers must be able to comply with the request without undue delay and in any case within one month of receipt of the request. If you implement a process to port data, you should implement a procedure to process other individuals' requests in accordance with law and provide extra services, for example by guaranteeing more data security.

ii) Aim for the competitive advantage. Think about developing a user-friendly tool or interface that involves the individual and gives them more transparency, insight and control over their own data than other competitors.

This right gives customers the ability to switch service providers more easily, make sure they transfer their personal data to your organization and not your competitor's.

"In our Top Ten series we highlighted ten subjects under the GDPR and elaborated on them to give you a good general basic understanding of those subjects."

GDPR: What controller/processor guarantees must be agreed?

Co-operate compliantly and effectively

Proactively identifying your controller/processor relationships, and updating the terms under which these relationships operate, will be critical to processing personal data compliantly. No detailed guidance is offered by EU authorities on what particular steps to take in such relationships, yet a minimum set of controller/processor guarantees must nevertheless be agreed upon in terms of the General Data Protection Regulation (GDPR). In this article we explore how the controller and the processor can co-operate compliantly and effectively under the GDPR.

By Rodney Mhungu and Marloes Dankert (Deloitte NL)

Identifying your controller/processor relationships

Just because a vendor you are working with needs to process personal data in order to provide you or your customers with a service, it does not automatically make that vendor a processor. It is important to assess the specific context of your relationship with each vendor in order to determine this, because in the ever-complex world of business, governance, and computing, there is no one-size-fits-all relationship when it comes to data processing.

A controller decides on the means and purposes of processing personal data. If you assess the factual situation of a data processing relationship, not only the contractual terms, you can find a number of factors which indicate that an organisation is exercising controllership, including that the organisation

- determines which data are processed
- determines the purposes for processing such data
- decides how long (personal) data should be retained
- has complete control over data access, and
- decides whether data will be transferred to a third party or be transferred to a third country outside the European Economic Area

On the other hand, a processor processes personal data on behalf of the controller. One crucial indicator of this is that a processor's core service is to process data on behalf of the controller. If the data processing is a mere result of other services provided, that is an indication that you are not dealing with a data processor. You may actually be dealing with a (joint) controller. For example, if one of your vendors is using your, say, web-shop performance data based on customer interaction to aggregate it against the vendor's other customers, and provides you an analytics report on that basis, your vendor is processing "your data" for its own business analytics purposes. These business analytics reports may be useful to you, but your vendor would be a controller in this situation, not a processor. As a result, the vendor would need its own lawful basis/bases for processing your data, if it only relies on your lawful basis for processing, you may both be in jointly liable for infringing the GDPR.

Processors must process personal data on written instructions from the controller.

Exposure to privacy risks

For the GDPR's provisions on processors to apply, the processor must process personal data on documented instructions from the controller. An overwhelmingly popular market trend to include processors under the umbrella of "third party" vendors in the vendor management process can lead to the misleading assumption that you can mitigate your GDPR risk with vendors by sending each (third party) vendor a data processing agreement geared towards establishing guarantees for a controller/processor relationship. However, if you do not identify the relationship with your vendor correctly, you may end up exposing your organisation to privacy risks you did not take into account, such as

- privacy risks related to a joint controller relationship: if your vendor turns out to be a joint-controller, by deciding on (an aspect of) the means of processing personal data that you process together, that vendor may be subject to the same controller obligations as you are, which means your relationship is subject to a different set of (shared) risks and responsibilities than those in a controller/processor relationship.
- privacy risks related to a controller-to-controller relationship: if you are sharing personal data with a vendor after you have decided on the means and purposes of processing personal data, and that vendor determines how or why to process that personal data once you have shared it, perhaps you are transferring personal data to another controller. Firstly, you would need to have a lawful basis to transfer this data to your vendor. And secondly, this relationship of continuous data sharing may better be catered for in a data transfer or data sharing agreement rather than a data processing agreement.

Presuming you have correctly identified your vendor as a processor, how do you manage that relationship?

How to manage the controller/processor relationship?

Processors may be better equipped than their controllers to have expertise and technology to maintain state of the art security measures, recall information necessary to respond to data subject rights, and provide effective methods for identifying or categorizing high risk data processing. In this respect, the GDPR requires processors to help controllers deliver on their data-intensive compliance obligations.

Nonetheless, as a controller you still need to have complete control over what personal data your processor processes (i.e. what it gathers, stores, manipulates, and transmits) on your behalf. This control essentially means directing what your processors do, and why.

Your processor may have more sophisticated data processing capabilities than you do, and perhaps that is why you hired the firm in the first place, but you will not be able to manage your risk effectively if you ask your processor to process personal data in ways your organisation is not yet equipped to absorb, utilize or understand. For instance, machine learning can bring about tremendous efficiencies, but computers learn best from high quality datasets supported by value-driven analytics and clear business processes to support those analytical insights; if you are still working on the quality of your data sets, learning how to derive value from your analytics, or you are working on business processes to absorb this value, you should not yet be asking your processors to deliver machine learning capabilities to your organisation.

Asking for machine learning when your organisation is not yet mature in analytics may lead to data processing for purposes you did not request or even foresee. Asks such as these, if important for the goals of your organisation, may be better suited for business venture partnerships in the form of joint-controller or controller-to-controller relationships.

Provided you do indeed have control over the data processed by your processor, three key practices should be initiated, developed and updated regularly for you to manage your controller/processor relationship compliantly:

- ensure all your instructions for the processor are documented in writing;
- vet your processors for GDPR compliance and the use of sub-processors to process personal data on your behalf; and,
- in collaboration with your processor, design privacy-enhancing techniques and operations for all your processing operations.

Conclusion

First of all, as a controller, make sure that you have correctly identified the processors in your organization as compared to other types of vendors. Secondly, stay in control of how your personal data is processed by each processor; no matter how technologically capable your processor is, you can only maintain this control if you can effectively absorb the value and mitigate the risks of the data processing. And thirdly, continuously manage your relationship with your processors, in order to work together towards a risk-based and effective approach toward protecting personal data.

GDPR and Industries: impact on Financial Services

Using transaction information under GDPR

Using customers' financial information is interesting for both the traditional financial services industry, as well as for newcomers. The General Data Protection Regulation (GDPR) strengthens the existing privacy rules, but also allows organizations to make use of personal data within these constraints.

By Annika Sponselee & Bart Witteman (Deloitte NL)

You are what you buy (maybe)
Google's search engine is often characterized as the ideal advertising information gathering machine: Google users type in exactly what they want at that moment. My search for 'black leather sneakers' likely means that I'm looking for new shoes. A good opportunity to show me where to get that great pair of new shoes.

Many consumer banks have transaction information available, which provides similar insights – with a small difference. Transaction data doesn't show the future what I want, but rather the past what I have spent my money on.

In part, this information seems less valuable: an advertiser may not want to know which items I have already purchased. On the other hand, this data may give good insights into my spending patterns and determine what I might want or need next. If I am spending a lot on furniture at a multinational home store, I may also be interested in some paint from a local DIY store in a color to match my new couch.

Know your customers – and what they want
The interest in this transaction data is large. The second Payment Services Directive (PSD2) will open up this information to service providers (when consumers consent). Startups, tech giants and more traditional financial organizations see this value and are looking to use the data where they can.

Consumers can also get advantages from newly developed services, as long as service providers find a mutual benefit for consumers and themselves. I'm happy to provide my transaction data in order to get offers sent to me, as long as I feel these offers are truly interesting to me instead of seemingly random and intrusive ads. Others may not like these offers – which is of course fine, as long as they are able to make a clear choice.

Providing consumers with this choice will be important. If a business model can't exist without this data use, at least give me the option not to use your service. The GDPR emphasizes giving the data subject the control and the power to make decisions.

To serve and protect
There are some constraints: I want to know in a fair amount of detail what my data is being used for. I want to have control over when I want the service to stop, and I want to be able to order the service provider to delete my data upon request. I also want to have this information and exercise my rights right now, not by sending a letter through the mail.

In addition: my data should never fall in the wrong hands. Traditional financial institutions have massive security budgets to protect the data concerning a customer's financials. Newcomers may find this to be more difficult.

Privacy constraints have existed for a long time. The GDPR clarifies many constraints and strengthens consumers' rights. Its message is clear: you can use personal data, as long as you have included sufficient safeguards to protect consumers' rights.

GDPR Update: a consumer product and retail perspective

Truly enabling your customer

This blog will provide guidance on some of the specific elements that should be taken into account when implementing the GDPR in the consumer products and retail sector.

By Richard Spoelstra (Deloitte NL), Christian Wernberg-Tougaard (Deloitte DK) and Thomas Tzieropoulos (Deloitte DK)

The consumer and retail industry is – beside governments – one of the industries that process the most personal data. This is why knowing the regulation and its impact is tremendously important. Implementing the GDPR is not only about compliance, not only about it-security, but is essentially about changing the culture – to become an organisation that asks questions like: 'Why do we collect these data?', and 'Do we have a legal base to do so?', in order to embrace privacy and protection of data. Furthermore, companies in the consumer products and retail business must maintain a high level of trust with their consumer base to retain brand loyalty – something that can be severely impacted by a privacy data breach.

Knowing your customer

To gain and keep this trust from your customers– and by in large because data privacy is about protecting the individual – you need first to understand your customer. Questions you will need to ask are not all that different from those your marketing department asks: "Who is my customer?", "What message do I want to convey to my customer?" and "What does my customer expect of me?"

Only by asking these and similar questions will your organisation get an idea of what your data privacy objectives are going to look like. Why? Because the GDPR, a risk based legislation, requires you to look at risk from an individual's perspective. This, unlike other risk based domains such as that of information security, which are mostly approached from an organisational risk perspective. As such, the GDPR requires you to adopt a different way of thinking.

Data privacy will be different for each organisation and even within your organisation for each channel, country, and region in which you operate. Customer centricity will therefore require you to know not just your business and your target group, but also the regional nuances and what data privacy means within that context. What is essential to protect in the Netherlands is not necessarily the same as that in Poland.

Customer Centricity

Because each customer group, and in some way each customer, is different; a customer centric data privacy approach will also be different for each organisation. Requiring a different level of effort and for each organisation to face their own unique set of challenges. How to approach privacy when you have an online business selling tickets for local jazz concerts will be entirely different from designing a customer centric data privacy program for an international brick-and-mortar retail chain. While this seems straightforward it happens all too often that a one size fits all solution is chosen.

In the end to be really customer centric, data privacy will have to be seamlessly integrated within the service you offer. Your customer should not be aware of the measures you are taking to protect the data. This will feel counterintuitive, because data protection revolves largely around being transparent. But it shouldn't be counterintuitive. You should still be transparent about how your organisation uses personal data. At the same time, your organisation should be designed in such a way that everything you do to protect data feels right to the customer.

What does this mean for your business?
To achieve this, and to go from a regulatory focused privacy approach to a customer focused privacy approach the way you approach privacy will need to change. The ownership and the design of privacy should shift to your operational departments. Instead of telling your departments that they need to do something a certain way, the approach taken should instead reflect an environment where you are assisting them in creating a better product.

Regulatory focused privacy is about showing compliance. It involves policies and procedures. Customer focused privacy takes this and makes it work for your organisation. It is about setting your organisation up to win and in the end, most importantly, about truly enabling your customer.

"In the end to be really customer centric, data privacy will have to be seamlessly integrated within the service you offer."

GDPR in the public sector

The biggest and smallest changes

The closer we get to May 2018, the louder we hear the rumble: The General Data Protection Regulation ('GDPR') is on its way. With stronger rights for data subjects and higher fines, the European Union intends to send out a strong message: privacy needs to be taken seriously. How will the changes that are coming relate to organisations in the public sector? We highlight a few topics to provide a better understanding.

By Esther van Duin (Deloitte NL)

Lesser known articles of GDPR
Starting May 25th 2018, all organisations, including those in the public sector, need to comply with the GDPR. Because of the broad scope and big consequences of this new regulation, plenty of articles and opinions have been published describing the possible consequences.

We see, however, that most of the available documentation focuses on general information and consequences even though for some sectors various parts of the GDPR are important. In the public sector several articles of the GDPR that are often described will be less applicable, whereas other, less described articles, will have a higher impact on the public sector specifically.

In order to create clarity in a time where up to date data protection knowledge is of utmost importance, we aim to describe some of the specific impacts the GDPR will have in the public sector. We will first demonstrate which of the commonly known (new) legal obligations of the GDPR have a smaller impact on the public sector compared to other fields. Then we will look into -lesser known- articles from the GDPR that will be applicable specifically to organisations operating in the public.

Changes that the GDPR brings
As explained, not all changes that the GDPR brings will have an equally big impact on organisations operating in the public sector. Several new obligations, such as data portability, will play a smaller role in this sector than on other sectors.

Data portability
The right to data portability is a good example of a much discussed new right for data subjects. This right for data subjects to retrieve personal data in a machine readable format needs to be supported by organisations when applicable. However, only personal information collected under consent, or in order to execute a contract qualifies to be subject to data portability. As organisations in the public sector most of the time cannot use freely given consent as a ground for data processing - for the government has a too strong of a position in relation to the data subject -, data portability will mostly only play a role in contractual relations. Since different grounds are often used for personal data processing within the public sector, than in the private sector, such as processing for performing a task of public interest, data portability will not play such a big role in the privacy landscape of the public sector.

Right to be forgotten
The right to be forgotten will also play a smaller role in the public sector, compared to other sectors. This is mainly a consequence of the grounds that the GDPR provides for when the right to be forgotten is not applicable: in case the processing happens for performance of a public interest task or exercise of official authority, or the processing is executed for compliance with a Union or Member State legal obligation, the right to be forgotten is not applicable. Both types of processing occur relatively often within the public sector.

One-stop-shop
Another new possibility the GDPR brings is the often quoted 'one-shop-stop'. This enables organisations that operate EU wide to only deal with one data protection authority, instead of dealing with each data protection authority per EU country they operate in. However, since organisations in the public sector often mainly operate in one country (the country that created the organisation), this possibility will not play as big a role for these organisations.

3 most important GDPR changes for the public sector
There are a number of provisions that are specifically relevant for the public sector that are likely to result in changes. We highlight the three most important ones.

Data Protection Officer
Government agencies that process personal data are always required to appoint a Data Protection Officer (DPO). This is different in the private sector, where a DPO is only required when certain criteria are met. It is possible to share a DPO with organisations or agencies, as long as the organisational structure and size are taken into account. Also, consult local legislation to determine if there are additional requirements, such as registration of the DPO in a government register.

Legitimate Interest as grounds for processing
The GDPR restricts the public authorities from using Legitimate Interest as a legal grounds for processing personal data. This means that public authorities must find another legal ground if Legitimate Interest is currently relied upon. Review the processing activities and determine if it can be processed under a different lawful basis, is exempted, or if a derogation applies. If this is not possible, the personal data may not be processed.

Consent for (international) data transfers
Consent is another legal ground for processing with restrictions for the public sector. The GDPR does allow a data transfer based on consent of the data subject, however, public sector organisations can hardly ever use this exemption. The rationale behind this is the relational imbalance between the government and its citizens, which is impeding with the requirement that consent must be 'freely given'. The GDPR does provide a special option for governmental bodies to exchange data with third countries without suitable safeguards. This is possible if there is a legally binding and enforceable instrument between the government authorities.

Conclusion
The GDPR draws special attention to protection of personal data in the public sector. It introduces a number of significant changes and restrictions. A careful assessment must be done as not all provisions are applicable. Especially the exceptions should be carefully considered before the general rule is applied. When doing so, we advise to also consult local legislation, because it may impose stricter or even additional requirements.

Contact

Annika Sponselee
Partner Risk Advisory
Global & NWE GDPR leader
Mail: asponselee@deloitte.nl
Tel: +31610999302

Nicole Vreeman
Manager Risk Advisory
Mail: nvreeman@deloitte.nl
Tel: +31882887717

Authors

Rodney Mhungu
Marloes Dankert
Annika Sponselee
Rodney Mhungu
Jan-Jan Lowijs
Nicole Vreeman
Alex Tolsma
Shay Danon
Sebastian le Cat
Robyn Post
Alexander Garrelfs
Michiel van Schaijck
Filipa Carmo Pedro
Ria Halme
Nathalie McNabb
Soeren Klaebel Clemmensen
Alex Tolsma
Pieter Lamens
Evelyn Caesar
Annika Sponselee
Bart Witteman
Richard Spoelstra
Christian Wernberg-Tougaard
Thomas Tzieropoulos
Esther van Duin

Deloitte.