GDPR Compliance Roadmap

bureau Brandeis

On 25 May 2018 the General Data Protection Regulation ("**GDPR**") comes into effect. From that date the GDPR will have a direct effect on all EU Member States, and must be complied with. The current Dutch Personal Data Protection Act ("**Wbp**") based on the Privacy Directive of 1995 (Directive 95/46/EC) will then cease to apply.

The GDPR radically alters the legal framework for the protection of personal data. It introduces new concepts, contains comprehensive new obligations for business, and strengthens the rights of data subjects (individuals whose data is being processed). Furthermore, the GDPR introduces hefty maximum fines of € 20 million or 4% of an organisation's global turnover.

The GDPR has implications for virtually every company or organisation not only in the European Union, but also beyond its borders. Given strict regulations combined with high fines, it is prudent for companies to be aware of the content of the GDPR at an early stage, and to prepare themselves accordingly.

Below we will show how our clients and business contacts can prepare for the GDPR as efficiently as possible in twelve steps. bureau Brandeis regularly assists parties with respect to the application of privacy legislation and has plenty of experience with the GDPR. Naturally, we will be happy to assist you with your preparations for the GDPR.

Disclaimer:
This document is intended as a guideline and is not intended as legal advice.

© bureau Brandeis, 2017

Ready for the GDPR in 12 steps

1. Appoint the persons responsible and – if necessary – a Data Protection Officer ("DPO")
2. Inventory personal data processing operations and make a gap analysis
3. If necessary, carry out a DPIA
4. Introduce a data minimisation policy (decide on your retention periods)
5. Establish a register/administration and document your processing operations
6. Update your security policy and apply Privacy by Design and Privacy by Default
7. Implement tools to respect the new rights of data subjects
8. Update your privacy policy
9. Draw up a data breach protocol and keep a register
10. Check your processors and data processing agreements
11. Update your registration flow to obtain lawful consent
12. Work out which supervisory authority you report to

© bureau Brandeis, 2017

STEP 1

Appoint the persons responsible and – if necessary – a Data Protection Officer (“DPO”)

© bureau Brandeis, 2017

To begin with, it is important to identify who, within your organisation, is responsible for privacy compliance and who else is involved. These are firstly individuals who are authorised to decide on important matters on behalf of the organisation, but also individuals who know about law, technology and data processing within an organisation. It is important that these people recognise the importance of privacy compliance.

What do you need to do?

- Organise a kick-off meeting or a number of meetings with the relevant individuals. These might include:
  - Management Board;
  - Policymakers;
  - Lawyers;
  - Other individuals that have a lot to do with personal data, such as HRM staff, customer services, the IT department, etc.
- Give them information about the GDPR and the importance of privacy compliance.
- Determine, in broad terms, the most important focus areas/risks for your organisation. This partly depends on your organisation's core activity.
- Determine who is responsible for privacy compliance and how the tasks will be divided. How will decisions be made? When and to what extent should the Management Board be involved? Who will be responsible for and/or involved in the implementation, etc.?

Data Protection Officer

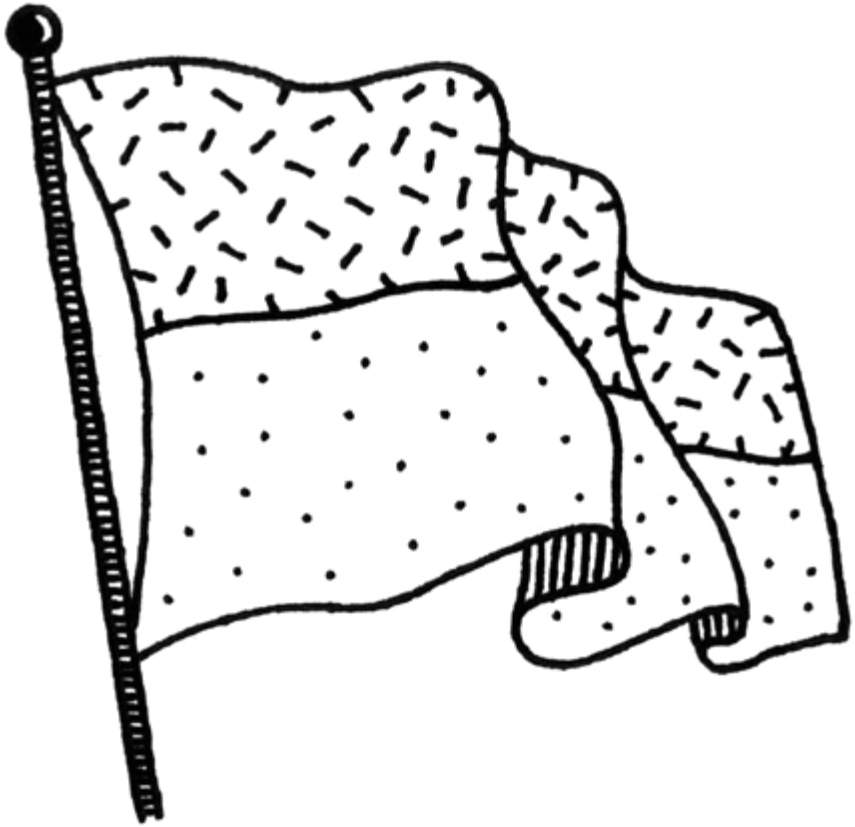
Under the GDPR your organisation may be obliged to appoint a Data Protection Officer or "DPO". Even if it is not obligatory, you can still appoint a DPO. Decide now whether your organisation needs one. In any case, you must appoint a DPO (i) if you are a public authority or body, (ii) if your work involves processing operations that amount to regular and systematic observation of individuals on a large scale, or (iii) if your job involves processing of special personal data on a large scale (see **Step 2**).

A DPO is a kind of internal supervisory authority. The DPO informs and advises the organisation about obligations under the GDPR and other obligations in the field of data protection, and ensures compliance with those obligations. He or she is also the organisation's contact person for the supervisory authority and for data subjects.

© bureau Brandeis, 2017

To perform these duties, the DPO should be an expert in the field of legislation and practice regarding the protection of personal data. He or she must also be given sufficient support and resources to implement this, and have a certain amount of autonomy.

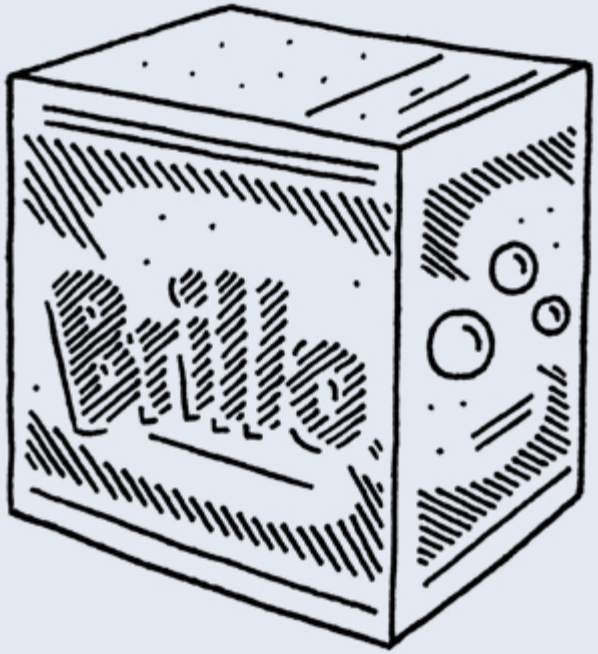
- Decide whether the appointment of a DPO is required or desired.
- Decide who should be the DPO and ensure that this person is sufficiently trained.
- Determine the scope of the DPO's duties and ensure he or she has sufficient support and resources.
- Appoint the DPO and register them with the Data Protection Authority.



© bureau Brandeis, 2017

STEP 2

Inventory personal data processing operations and make a gap analysis



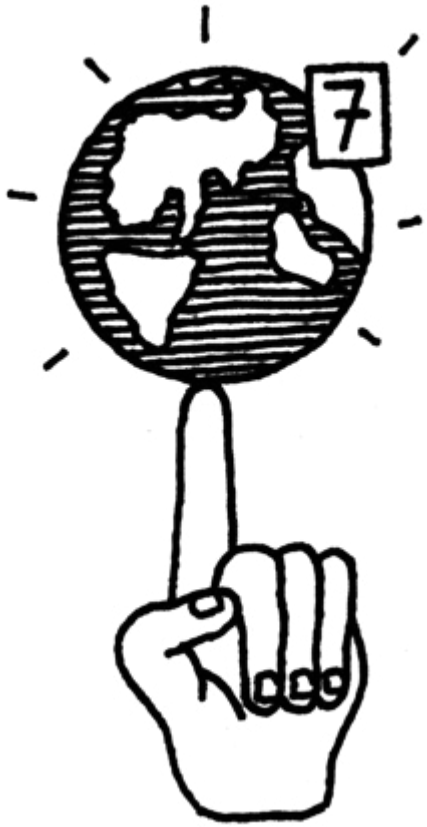
© bureau Brandeis, 2017

To be able to act in accordance with the GDPR, you must firstly inventory the personal data processing operations within your organisation. You should know which data is used, by whom and for what purposes. Then you can assess what needs to be changed in order to be compliant by 25 May 2018.

Answer the following questions:

- Which personal data is processed within the organisation?
  - Which data? For example:
    - Name;
    - Adress;
    - Job title;
    - Contact details (which?);
    - Assessments;
    - Travel details, etc.
  - From which categories of data subjects? For example:
    - Clients;
    - Employees;
    - Suppliers;
    - Visitors;
    - Patients;
    - Travel details, etc.
- Do you process “special categories” or other sensitive data? For example:
  - Data concerning health;
  - Biometric data (e.g. fingerprints);
  - Citizen Service Numbers (*BSN*);
  - Data relating to minors;
  - Profiles.
- Are there any other special risks?
  - Do you combine data, use profiles or are any automated decisions made?
- For what purposes are the various data used?
- On what legal basis?
  - Will this remain valid under the GDPR?
- Who is processing the data and who are you sharing the data with?

© bureau Brandeis, 2017



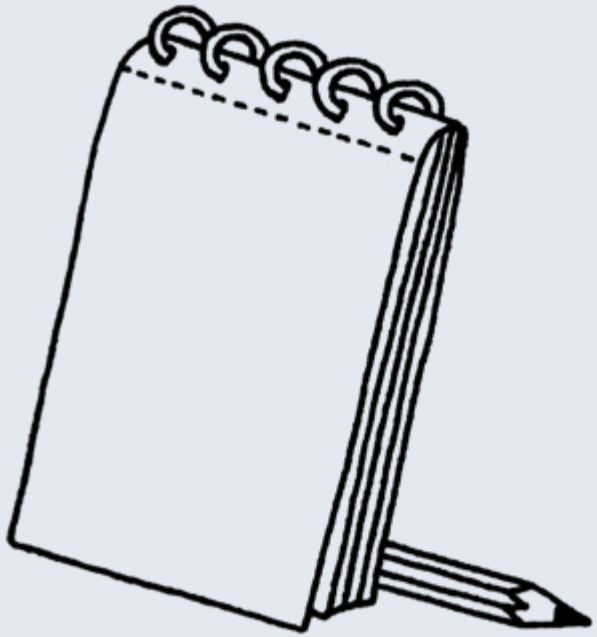
- What information is given to the data subjects? For example:
  - A privacy policy;
  - A code of conduct for employees.
- Is there a process for inspection, correction and deletion, etc. of personal data?
- Which service providers are involved in the (further) processing of personal data?
  - Are there any data processing agreements?
- Is there a security policy?
- Do you practise Privacy by Design and Privacy by Default?
- Is there a data breach protocol?

Having answered the questions above, you will have a better idea of the data processing operations within your organisation, the greatest risks associated with those operations, and what will change for you. You can then decide what action to take before 25 May 2018 and which subjects are a priority for your organisation.

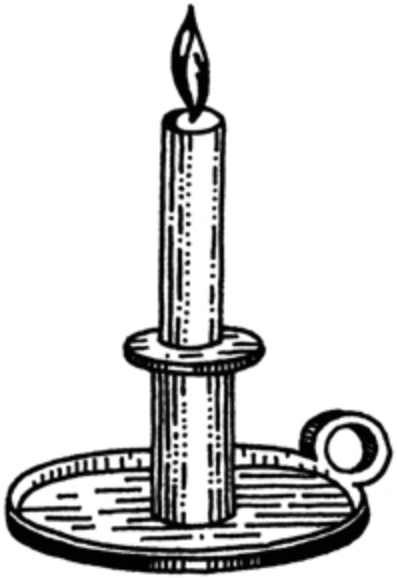
© bureau Brandeis, 2017

STEP 3

If necessary, carry out a DPIA



© bureau Brandeis, 2017



Under the GDPR you may be obliged to carry out a data privacy impact assessment ("**DPIA**"). A DPIA is an instrument that allows you to inventory a data processing operation before such operation is carried out, so that measures can be taken to reduce those risks.

When is there a need for a DPIA?

A DPIA is mandatory for (envisaged) data processing operations which, given their nature, context and objective, represent a high risk to privacy. There is certainly a high risk in the following cases:

- If you assess individuals on the basis of personal characteristics and base decisions on those characteristics. This includes profiling and forecasting;
- If you process sensitive personal data, such as data regarding health, data on crime or political preferences, on a large scale;
- If you monitor people in public places systematically and on a large scale (e.g. camera surveillance).

In all other instances you must decide for yourself whether an operation entails a "high risk". If your processing operation meets two or more of the following criteria, you can assume that you must carry out a DPIA:

- You make profiles of people;
- You make automated decisions that materially affect the data subject;
- You conduct systematic monitoring on a large scale;
- You process sensitive personal data;
- You conduct data processing on a large scale, i.e. processing that involves many people, a lot of data, a long period of time or a large area;
- You link up or combine different data collections;
- You process data relating to vulnerable persons, such as children, employees or patients;
- You are using new technology, e.g. Internet of Things (IoT) applications;
- You pass on personal data to countries outside the EU;
- The data processing operation means that persons cannot exercise a right, use a service or enter into a contract.

The Data Protection Authority will publish a list of processing operations for which a DPIA is mandatory.

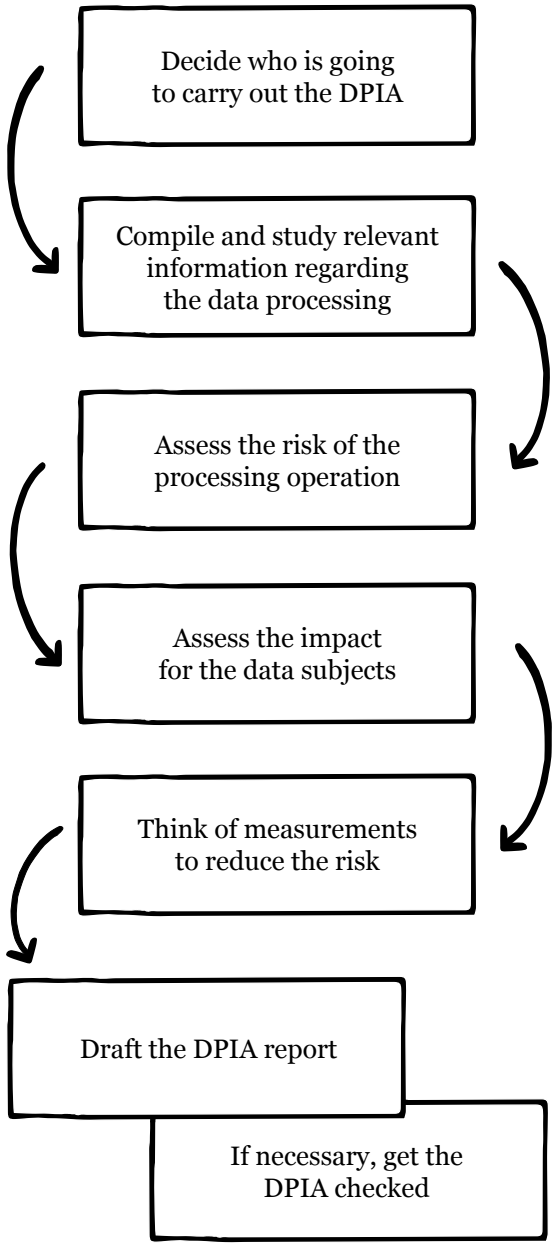
© bureau Brandeis, 2017

How should I carry out a DPIA?

You may choose for yourself how to carry out the DPIA, but it must always include the following:

- A systematic description of the envisaged data processing operations and the purposes of those operations. If you rely on a legitimate interest as a basis for the processing, you should also explain this interest in the description.
- An assessment of the need and proportionality of the processing operations. Is the processing operation necessary in order to achieve your goal? And is the breach of privacy of the data subjects not disproportionate in relation to this goal?
- An assessment of the privacy risks for the data subjects.
- The proposed measures to (I) tackle risks (such as pseudonymisation) and (II) demonstrate that you comply with the GDPR.

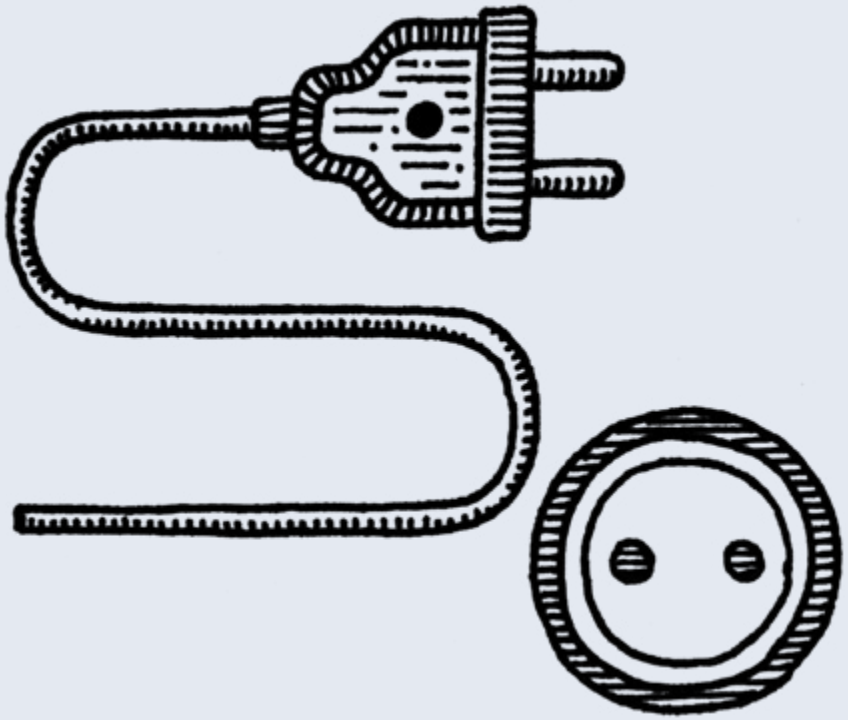
Has a DPIA revealed that your envisaged processing represents a high risk? And are you unable to find measures to limit this risk? In that case, you must discuss matters with the Data Protection Authority before you start the processing operation. This is called a prior consultation. Assess at this stage whether you should carry out DPIAs, and do so. If you make an early start, it will also be easier for you to comply with the other obligations under the GDPR.



© bureau Brandeis, 2017

STEP 4

Introduce a data minimisation policy (decide on your retention periods)



© bureau Brandeis, 2017

The GDPR emphasises the obligation not to process more personal data than necessary. This is also referred to as data minimisation. In this context it is important to determine how long you will retain the personal data and ensure that data is removed promptly.

What do you need to do?

- Based on the overview you have created of the various data (see **Step 2**), determine what purposes you are using this for and how long you should retain it for those purposes.
  - Is there a maximum or minimum statutory retention period (for each type of document/information)? For example:
  - Personal data from job applicants: maximum 4 weeks after the end of the application process;
  - Employment contracts for employees: maximum 2 years after the end of employment;
  - Income tax declarations and copy of ID for employees: minimum 5 years after the end of employment;
  - Recordings from CCTV: maximum 4 weeks after the recording has been made.
  - Is there a need for personal data to be retained? Can certain data be deleted from the data set perhaps?
  - Can the data be pseudonymised?
- Determine the retention period, the starting point for the time limit, and how the retention period will be enforced.
  - Make working arrangements regarding, for example, when and how hard copy documentation is archived (e.g. at the end of every month in a folder with date and destruction date) and who will destroy it;
  - Perform settings for (technical) archiving or deletion for each application/database, including settings for the deletion of archived data.

© bureau Brandeis, 2017

STEP 5

Establish a register of your processing operations

© bureau Brandeis, 2017

The GDPR introduces obligations for organisations to be clearly and fully responsible and accountable for the way in which personal data is handled. You must be able to demonstrate that your organisation is acting in accordance with the GDPR. As part of this you must keep a register of all processing activities that take place within the organisation, or under the responsibility of the organisation. Supervisory authorities can demand inspection of this registration.

You can use the overview that you created in **Step 2** as a basis for this.

The following data must be recorded in the register:

- Name and contact details of the person responsible (referred to in the GDPR as the "controller");
- Name and contact details of representative and/or DPO, if applicable;
- Processing purposes;
- Categories of data subjects;
- Categories of personal data;
- Any recipients;
- Transfers, if applicable, including name of the entity or person to whom the data is being transferred and documentation relating to appropriate guarantees;
- Retention periods;
- A general description of the technical and organisational measures for security.

Therefore, be sure to establish such a register and keep it updated. This may be through implementation of a data-mapping application, but also, for example, by maintaining an overview in an Excel file.

There are other different tools on the market which can help you to comply with this obligation.

Please note: the obligation does not apply to organisations with fewer than 250 employees, but does apply if (i) the processing operation presents a risk for data subjects (ii) the processing operation is not incidental or (iii) special categories of data are being processed.

© bureau Brandeis, 2017

STEP 6

Update your security policy and apply Privacy by Design and Privacy by Default

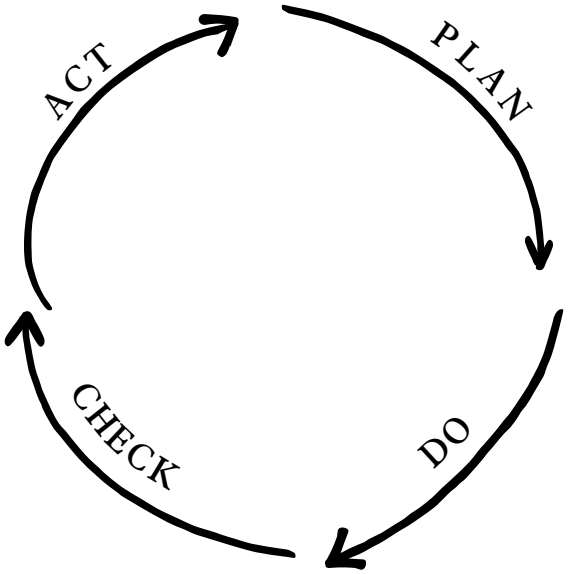
© bureau Brandeis, 2017

Under the GDPR you must take "appropriate technical and organisational measures" to secure personal data. What is appropriate depends on the processing risk. You must be able to demonstrate that you have taken appropriate measures and are able to make your considerations in this regard readily comprehensible. It is partly for that reason that it is important to check whether your security policy is still compliant and to update it where necessary.

In addition, the GDPR introduces obligations in the field of Privacy by Design and Privacy by Default. This means that as soon as you have chosen a medium for data processing or when designing systems or applications, you must take the personal data protection into account by implementing security measures and data minimisation, for example. The standard settings must be such that only personal data is processed for a specific aim. The rights of those concerned must be taken into account at all times as well, which includes in the design of a processing operation.

What you need to do:

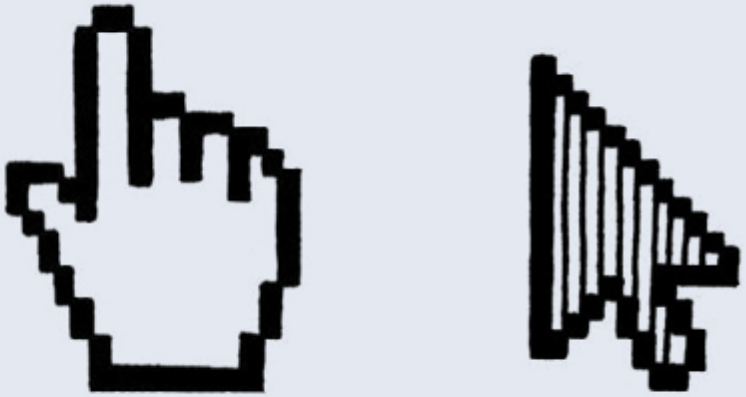
- For each type of processing operation, inventory the organisational and technical security measures you will take or have taken;
- Assess whether, given the risk of the processing and the state of the art, this is (still) adequate;
- Investigate whether data can be pseudonymised or encrypted;
- Check whether processing operations and/or retention periods can be restricted;
- Check whether measures have been implemented to guarantee the rights of data subjects (see **Step 7**);
- Implement additional measures where necessary;
- Decide when to test and evaluate your security measures;
- Set up a security policy describing the measures, your deliberations, and the periodic evaluation.



© bureau Brandeis, 2017

STEP 7

Implement tools to respect the new rights of data subjects



© bureau Brandeis, 2017

The GDPR gives particular attention to the rights of data subjects. For example, data subjects have the right to access and rectify their details. Moreover, individuals are being given even more opportunities to speak for themselves when it comes to the processing of their data. Their rights are being strengthened and expanded.

The GDPR introduces a number of new rights, such as:

- The right to receive comprehensive information, with the GDPR specifying which information must be improved in any event (see **Step 8**);
- The right to object to profiling and automated decision-making;
- The right to be forgotten. Under certain circumstances individuals have the right to have their personal data deleted. If an organisation has published data (e.g. posted it on the internet), reasonable measures must even be taken to pass the request for deletion through to all other organisations that process the data (obligation to forward);
- The right to data portability, or transferability of personal data. Individuals obtain the right – subject to conditions – to receive their personal data in a standard format, so that this can be easily passed on to another supplier of a similar service. For example, if they want to unsubscribe from one social network site and subscribe to another. They may even ask the organisation to send their personal details directly to the new service provider, if this is technically feasible;
- The right to restrict the processing of personal data;
- The right not to be subjected to exclusively automated decision-making, such as profiling;

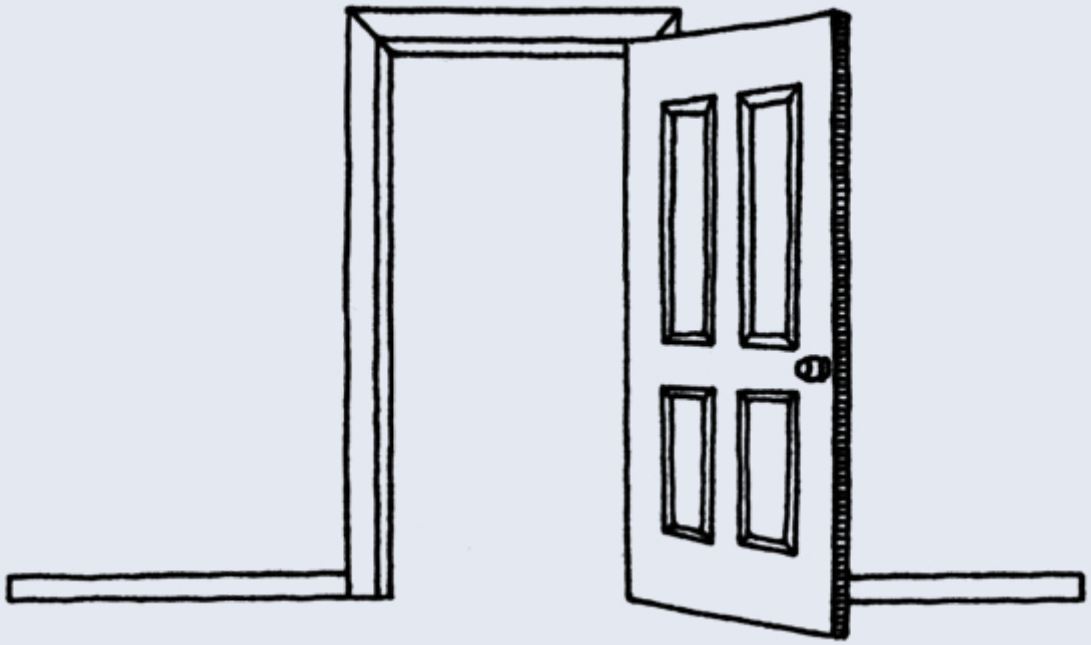
The GDPR also contains a separate provision regarding consent, of which more in **Step 9**.

You can see that there are a lot of new rights, which you must respect. Therefore, evaluate your procedures for granting access, etc. and set out the conditions for individuals to exercise their rights under the GDPR within your organisation. Determine whether it is appropriate to develop technical resources for that within your organisation, as in the context of data transfer, for example. These may include download programs to allow individuals to download their data easily and the provision of application programming interfaces (APIs).

© bureau Brandeis, 2017

STEP 8

Update your privacy policy



© bureau Brandeis, 2017

Under the GDPR you must inform data subjects about the processing of personal data. The information must be concise, transparent, understandable and easily accessible.

Under the GDPR you are obliged to provide information regarding, among other things:

- Your identity and contact details, and if possible, those of the DPO;
- The purposes of the processing and the legal basis for those purposes;
- The categories of personal data you are processing;
- The period that personal data will be stored (see **Step 4**);
- The rights of the data subject, such as the right to lodge a complaint, the right of access, rectification and erasure, and the right to withdraw consent at any time (see **Steps 7** and **11**);
- The source of the data;
- Any recipients or categories of recipients of personal data;
- Whether data is transferred to countries outside the EU;
- If applicable: which legitimate interest is served by the processing;
- Whether you practise profiling and, if so, how the data subject is affected by it;
- Whether the data subject is obliged to provide the personal data and what the consequences are of not providing that data.

The GDPR also provides for the future use of standardised icons so that information can be provided to consumers in a simple fashion.

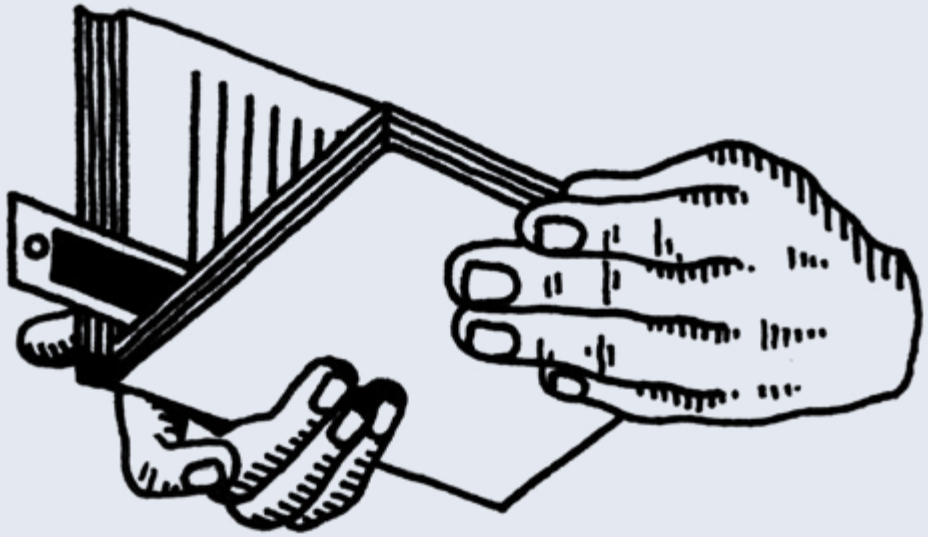
The information should, in principle, be provided at the time the personal data is collected.

Time, then, to update your privacy policy, in order to implement the additional information obligations that the GDPR is introducing.

© bureau Brandeis, 2017

STEP 9

Draw up a data breach protocol and keep a register



© bureau Brandeis, 2017

Under the GDPR you may be obliged to report a data breach to the competent authority and/or the data subjects. A data breach refers to the access to or destruction, alteration or release of personal data to an organisation without this being intended. Data breach therefore covers not only the release (breach) of data, but also unlawful processing of data and unintentional destruction. This might include a lost USB stick containing personal data, a stolen laptop, a breach of a data file by a hacker, or a fire, causing a CRM database (with no back-up) to be lost.
Under the GDPR you are obliged to report any data breach to the supervisory authority without delay, within 72 hours where possible. This is not necessary if it is unlikely that the data breach constitutes a high risk for the rights and freedoms of natural persons. The data subject must be informed if the data breach is likely to result in a major risk for the rights and freedoms of individuals, otherwise there is no need.

Data leak protocol

To be able to comply with the aforementioned obligations, you must ensure that (i) you are aware of a data breach as soon as it occurs and (ii) take appropriate action immediately. For this first point you must ensure that you implement measures to flag up data breaches as part of security (see **Step 6**). For the second point it is important to have a data breach protocol. In the protocol you can record (i) the steps to be taken if your organisation is confronted with a data breach, (ii) what information must be collected/recorded and/or reported, (iii) by whom, and (iv) within what time frame.

Also, make clear arrangements with your processors regarding data breaches. Find out what is included in the data processing agreement regarding data breaches (see also **Step 10**).

Data breach register

In addition, the GDPR imposes the requirement that all data breaches – both reported and unreported – that have occurred in your organisation, be documented in a register. Based on this, the competent authority can check whether you have complied with your reporting obligation.

Make sure that for each data breach you record the following information:

- Facts and details regarding the nature of the data breach;
- The categories of the individuals affected and – where possible – the number of data subjects;
- The (likely) impact of the data breach;
- The measures that your organisation has taken to tackle the data breach and limit its impact;
- Has the data breach been reported to the Authority?
- Has the data breach been reported to the data subject? If yes, include the text of the notification given to the data subject in the overview.

© bureau Brandeis, 2017

STEP 10

Check your processors and data processing agreements

© bureau Brandeis, 2017

A processor is a third party that processes personal data on behalf of an organisation. These may include service providers who do the payroll accounting, but may also include all kinds of cloud or other IT services where the service provider stores or can access your personal data.

You are obliged to enter into an agreement with each processor. Among other things, the agreement must include the fact that the processor:

- Will only process personal data on your instructions;
- Will take appropriate technical and organisational security measures;
- Will impose a duty of confidentiality on the individuals charged with processing personal data;
- Will provide assistance in the compliance with obligations pursuant to the rights of the data subjects;
- Will delete the data or return it to the controller after it has been processed;
- Will make available information that is necessary for audits or inspections by supervisory authorities.

So, now is the time to check your agreements with processors and possibly renegotiate them.

- Inventory your processors;
- Check whether your agreements comply with the GDPR;
- Where necessary, amend the agreements or enter into new data processing agreements.

In addition, the GDPR contains a large number of obligations for the processor. For example, under the GDPR processors must:

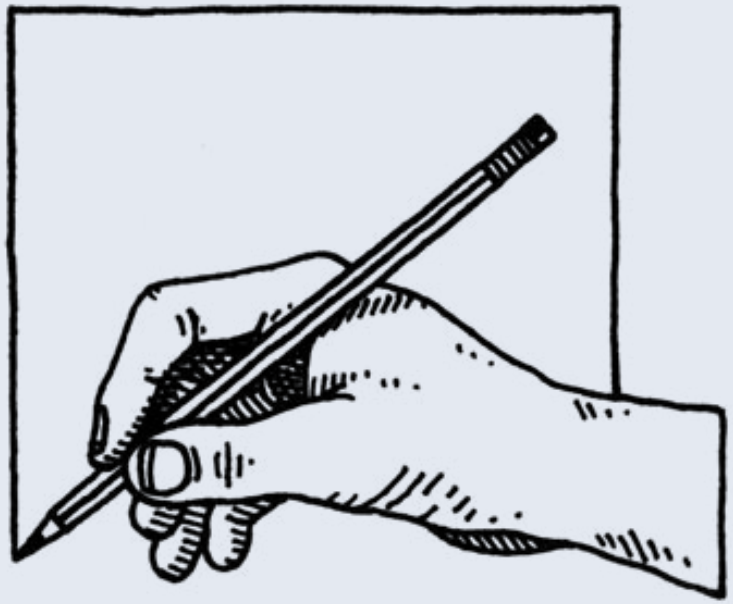
- Establish a register of all processing operations (see **Step 5**);
- Appoint a DPO if necessary (see **Step 1**);
- Seek permission from the controller for appointing sub-processors;
- Report data breaches to the controller;
- Cooperate with the supervisory authority;
- Act in accordance with the requirements for transfer of personal data to countries outside the EU;
- Carry out DPIAs (see **Step 3**).

Despite these obligations arising from the GDPR, it is advisable to discuss the points with your processors and determine by mutual agreement how these will be implemented in practice.

© bureau Brandeis, 2017

STEP 11

Update your registration flow to obtain lawful consent



© bureau Brandeis, 2017

A number of your data processing operations will probably be based on the principle of consent.

Lawful consent only applies if this is "freely given, specific, informed and unambiguous", without coercion. This can be given by means of a statement or an affirmative act, such as ticking a box, if sufficient information is also provided. The automatic, implicit assumption of consent or the use of pre-filled tick boxes is not sufficient to obtain valid consent.

Consent under the GDPR is not "freely" given if the data subject does not really have a choice, i.e. he is unable to refuse, or if it prejudices him to withdraw the consent. This may be the case if the conclusion of an agreement, including the provision of a service, depends on the consent of the data subject to process personal data that is not required for the performance of the task. Consent is also not "freely" given if no separate consent can be given for different data processing operations, even though this would be appropriate in the individual case.

You must be able to demonstrate that you have obtained the valid consent of data subjects to process their personal data.

Furthermore data subjects are entitled to withdraw their consent at any time. This must be as simple as giving consent, and before data subjects give their consent, they must be informed of this right. Otherwise consent is invalid.

If you process special personal data, the consent (subject to the applicability of an exception) must be "explicit". That means that the data subject must have explicitly expressed his will in words, writing or behaviour.

What do you need to do?

- Determine which processing operations are based on the principle of consent (see **Step 2**);
- Check whether the way you ask for, obtain and register consent is GDPR-compliant;
- Update your processes if necessary;
- Ensure also that data subjects can withdraw their consent easily.

© bureau Brandeis, 2017

STEP 12

Work out which supervisory authority you report to

© bureau Brandeis, 2017

The GDPR works on the basis of a "one-stop-shop".

The idea is that you deal with one supervisory authority, even if your organisation has establishments in several EU countries or if your data processing operations have an impact in several EU countries. This supervisory authority is called the "lead supervisory authority".

The lead supervisory authority is the supervisory authority of the EU Member State where the main establishment (or the only establishment) of the organisation is based. This is the place where the controller's central administration in the EU is situated. This is different if the decisions regarding the purposes and means of personal data processing operations are made in another establishment. In such event, that other establishment is the main establishment. For processors, the main establishment is the establishment where the central administration is based, or – if there is no central administration – the establishment where the main processing activities take place.

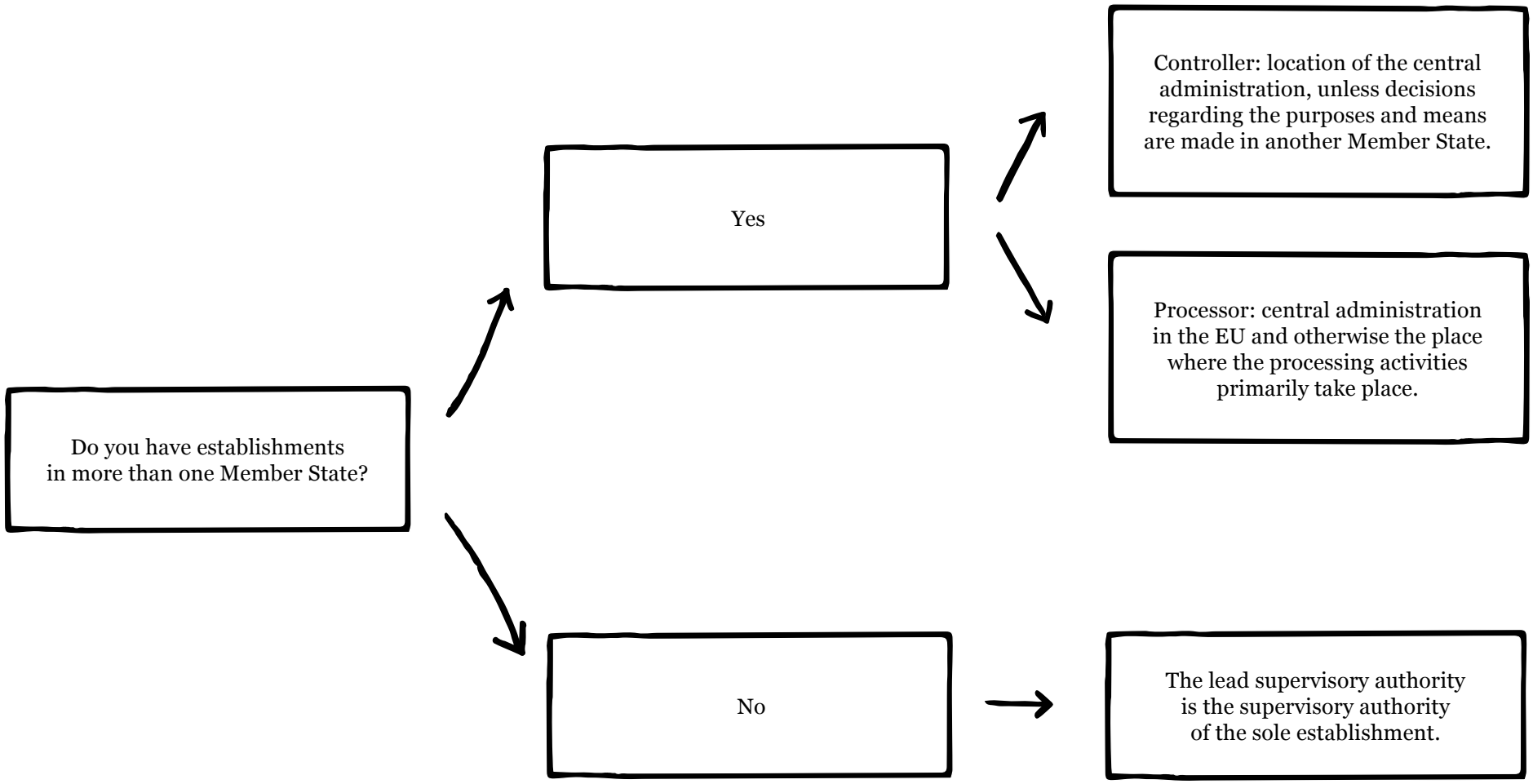
The lead supervisory authority is primarily responsible for supervision of organisations with cross-border data processing operations. The lead supervisory authority may also take on an enforcement role in cross-border processing operations of the organisation it supervises.

If a processing operation only takes place in a Member State other than that of the lead supervisory authority, or if a processing operation has a material impact on data subjects of that Member State, then a complaint can also be lodged with the supervisory authority of the Member State concerned. This supervisory authority – the "supervisory authority concerned" – must, however, inform the lead supervisory authority immediately and cooperate with it.

On the flip side, the lead supervisory authority must coordinate its actions with privacy regulators in other EU countries where the data processing has an impact. The lead supervisory authority coordinates the activities, involves the other supervisory authorities concerned in the matter and submits draft decisions to them.

Is your main establishment in the Netherlands? In other words: do you make decisions regarding the purposes of and the means for the processing operations in the Netherlands? Or do you only have an establishment in the Netherlands? Then you fall under the supervision of the Dutch privacy regulator, the Data Protection Authority.

© bureau Brandeis, 2017



© bureau Brandeis, 2017

The bureau Brandeis privacy team

Vita Zwaan

Christiaan Alberdingk Thijm

Silvia van Schaik

Marieke Berghuis

Caroline de Vries

Lex Keukens

Esther Janssen

Maartje de Graaf

Oskar Mulder

© bureau Brandeis, 2017

The name of our firm is a tribute to Louis D. Brandeis (1856- 1941), top-level American lawyer and judge in the US Supreme Court. Brandeis was one of the founders of the right to privacy.

Privacy requires special knowledge and expertise. It is an area of law that is constantly developing and enjoys wide public interest. As a result of the continual technical developments, our experts are always being asked to point these out and incorporate them into the stringent rules that regulate our dealings with personal data. This means we are in a position to assist and advise our clients in all phases of the development and implementation of privacy protection measures. The quality of our compliance department is unparalleled. No other firm has as much experience in the field of privacy litigation.

Thanks to our specialist knowledge and extensive litigation experience, bureau Brandeis is in an unrivalled position when it comes to preventing or resolving disputes with supervisory authorities or third parties. Thanks to our knowledge of all facets of the market we are able to see the playing field and together with our clients develop a strategy for the longer term. At bureau Brandeis we always develop our compliance work in close cooperation with our clients. Together we analyse the subjects that are of interest, draw up a plan of approach and steer the process within the company or organisation.

In the context of a compliance process various tasks can be performed, such as written advice, but also, for example, hosting practical workshops for our clients' staff, overseeing contact with supervisory authorities, drafting new policy and developing new internal procedures. Our advice is always practical and directly applicable within all layers of the organisation. Working together with our clients, we will make sure their organisations are privacy-compliant.

bureau Brandeis

Sophialaan 8-10 1075 BR Amsterdam Nederland
+31 (0)20 7606505 info@bureaubrandeis.com
bureaubrandeis.com