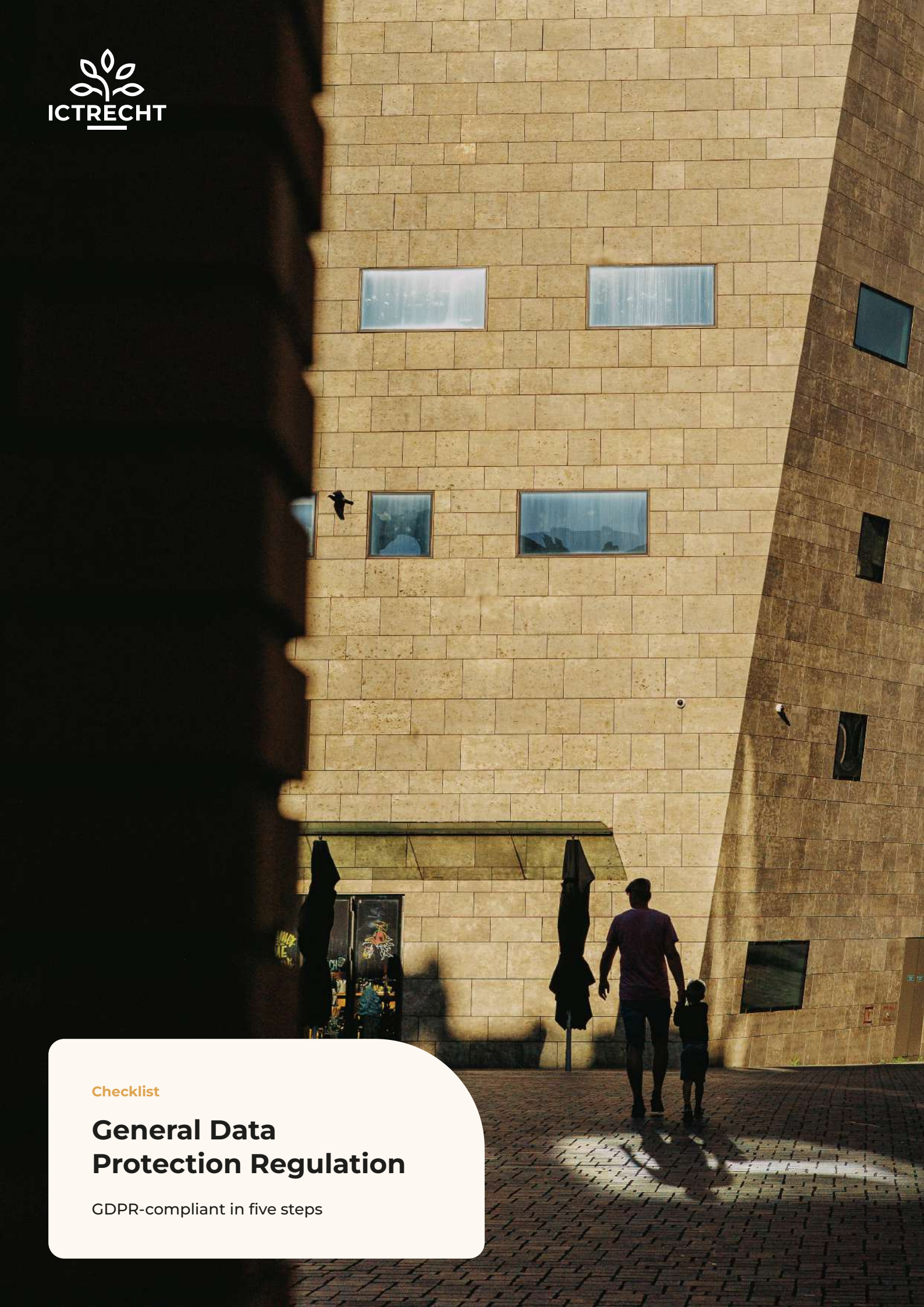
ICTRECHT



Checklist

General Data Protection Regulation

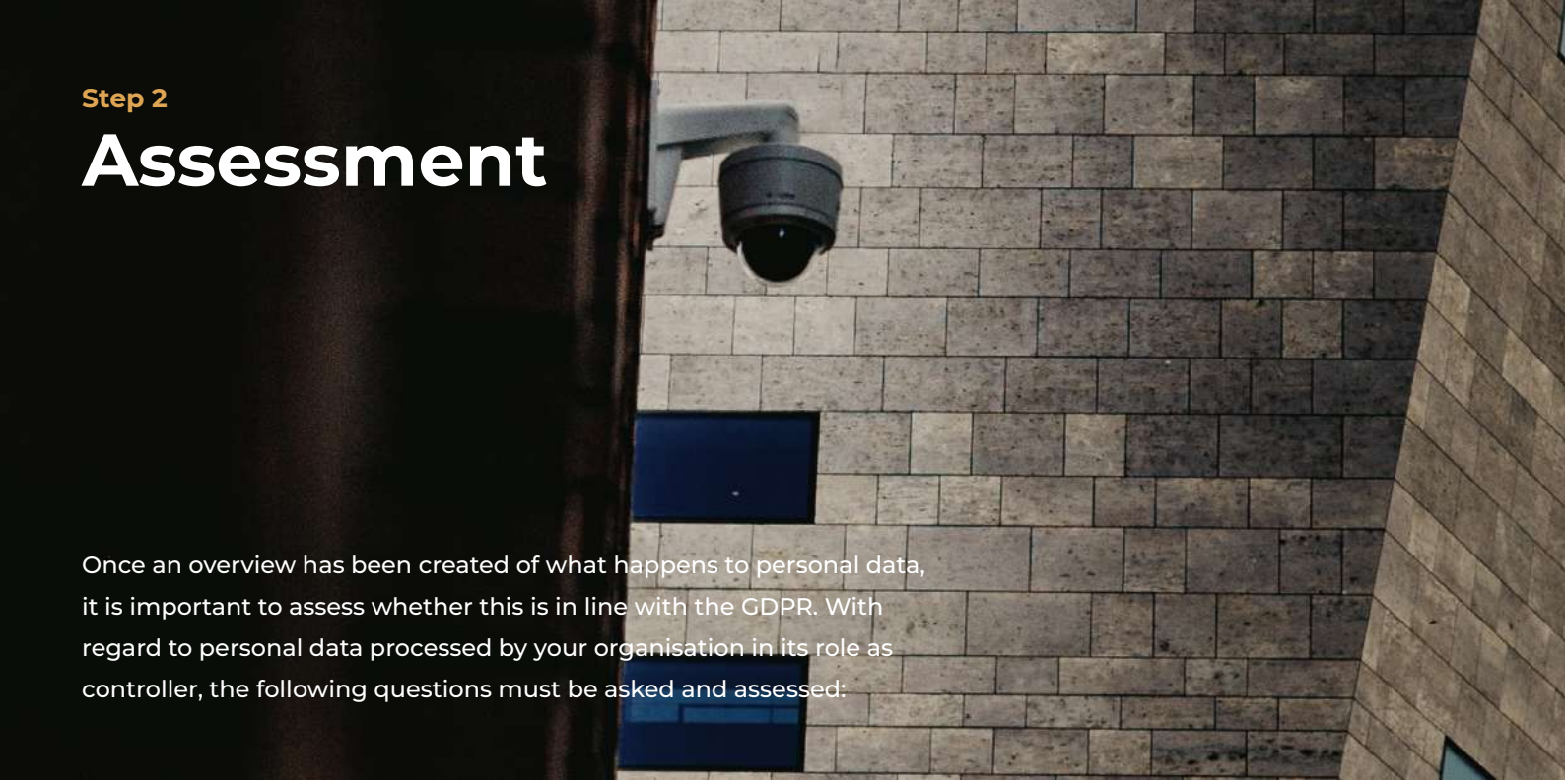
GDPR-compliant in five steps

Step 1

Inventory

Before implementing the GDPR, an overview must be obtained of the current situation regarding the handling of personal data. To do so, the following must be mapped:

Map out	Examples	Check
Through which channels personal data enters your organisation.	Website, cookies, customer assignments or employment contracts.	◯
Which personal data is processed.	Name, address, contact details, financial data or salary data.	◯
Whether special categories of personal data are processed and, if so, which ones.	Medical data, data concerning sexual orientation or religion.	◯
The data subjects from which these (special) personal data originate.	Website visitors, customers or employees.	◯
For which purposes these data are used.	Providing products and services or paying salaries.	◯
On which legal bases personal data are processed.	Performance of a contract or consent.	◯
Where and for how long personal data are stored and why that retention period is applied.	CRM system, up to seven years after the end of the (purchase) agreement.	◯
To whom and in what manner these personal data are disclosed.	ICT service providers, payroll administrators or other entities within the group.	◯
How the personal data are secured.	Passwords, secure connections or encryption.	◯
In which countries the personal data are processed, and therefore accessible.	The Netherlands, Germany or the United States.	◯



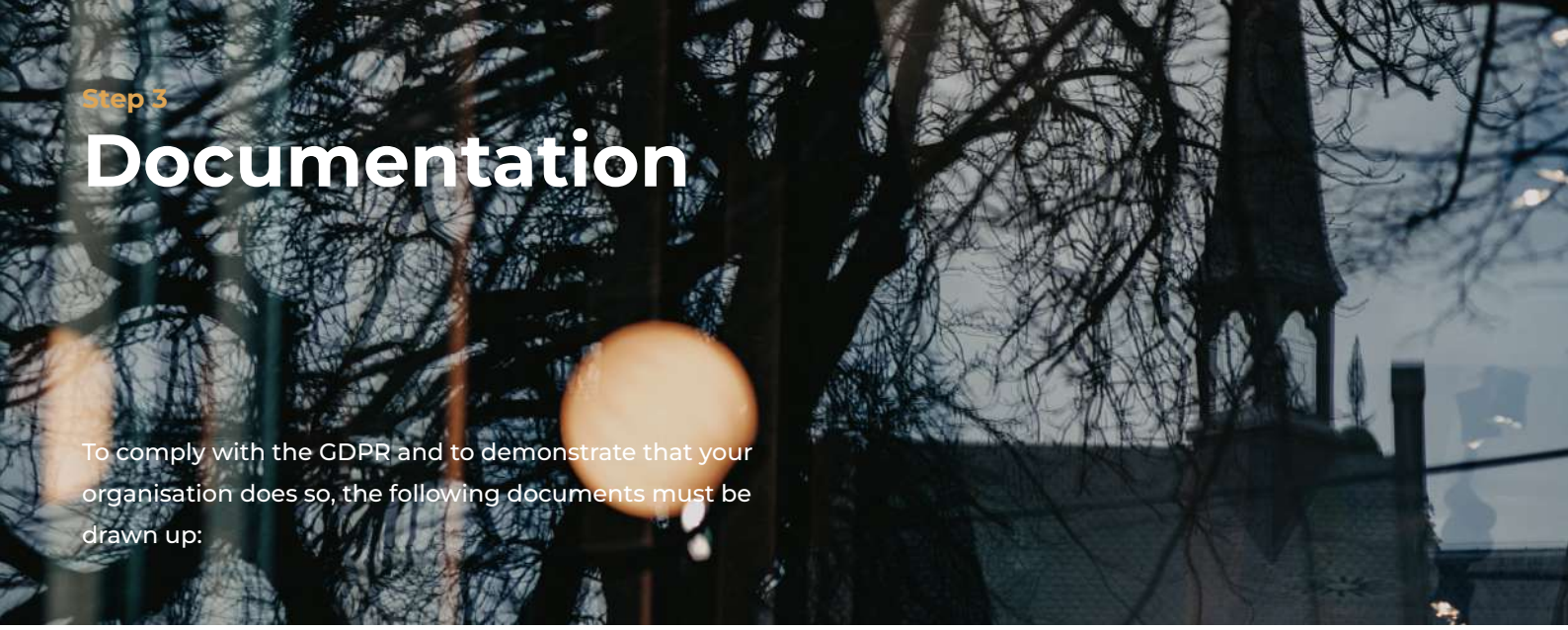
Step 2

Assessment

Once an overview has been created of what happens to personal data, it is important to assess whether this is in line with the GDPR. With regard to personal data processed by your organisation in its role as controller, the following questions must be asked and assessed:

Assess	Explanation	Check
What is our purpose and which data do we collect for this purpose?	Purpose limitation: personal data may only be used for the purpose for which they were collected, or for a purpose closely related to it.	◯
Do we have a lawful basis for the data we collect?	Lawful basis: personal data may only be processed if there is a lawful basis.	◯
Have we adequately informed data subjects about our data processing, for example through a privacy notice?	Information obligation: all data subjects must be informed about the processing of their personal data. At a minimum, information must be provided about the type of personal data, the purposes, the legal bases and the rights of data subjects.	◯
Do we collect only the data that are necessary?	Data minimisation: no more personal data may be processed than is necessary to achieve the defined purposes.	◯
Are the personal data we process still accurate, or are they possibly outdated?	Accuracy: personal data must be accurate and, where necessary, kept up to date.	◯
Do we store personal data only for as long as necessary for the purpose for which they were collected, and have we adopted a policy for this?	Storage limitation: personal data may not be retained longer than necessary. For certain processing activities, retention periods follow from the law, such as statutory tax retention obligations. Where no statutory retention period applies, an appropriate retention period must be determined.	◯

Assess	Explanation	Check
Have we made proper arrangements with all parties with whom we share personal data regarding how these data are handled?	Agreements: between controllers and processorand between processors and sub-processors, a processing agreement or sub-processing agreement must be concluded. Between two joint controllers, a data sharing agreement must be concluded.	◯
Are appropriate safeguards in place when personal data are processed outside the European Economic Area (EEA)?	Transfers: appropriate safeguards must be in place for the processing of personal data outside the EEA.	◯
Do we secure personal data in an appropriate manner?	Adequate security: appropriate technical and organisational measures must be taken.	◯
Are we able, upon request, to provide access to, rectify, erase, restrict the processing of and transfer personal data, and do we offer data subjects the possibility to object?	Rights of data subjects: data subjects have various rights under the GDPR. As a general rule, requests must be complied with within one month.	◯
Do we comply with the principles of privacy by design and privacy by default?	Privacy by design: privacy compliance is considered when designing or procuring systems. Privacy by default: default settings are privacy friendly.	◯
Can we demonstrate compliance with all of the above points?	Accountability: your organisation must be able to demonstrate compliance with the GDPR, including through its records of processing activities and the documents referred to in step three.	◯
Have we designated an internal point of contact (privacy officer) for GDPR compliance, or a Data Protection Officer (DPO) where required?	Point of contact: internally, it must be clear who is responsible for GDPR compliance, the so-called privacy officer(s). In addition, some organisations are required to appoint a DPO.	◯



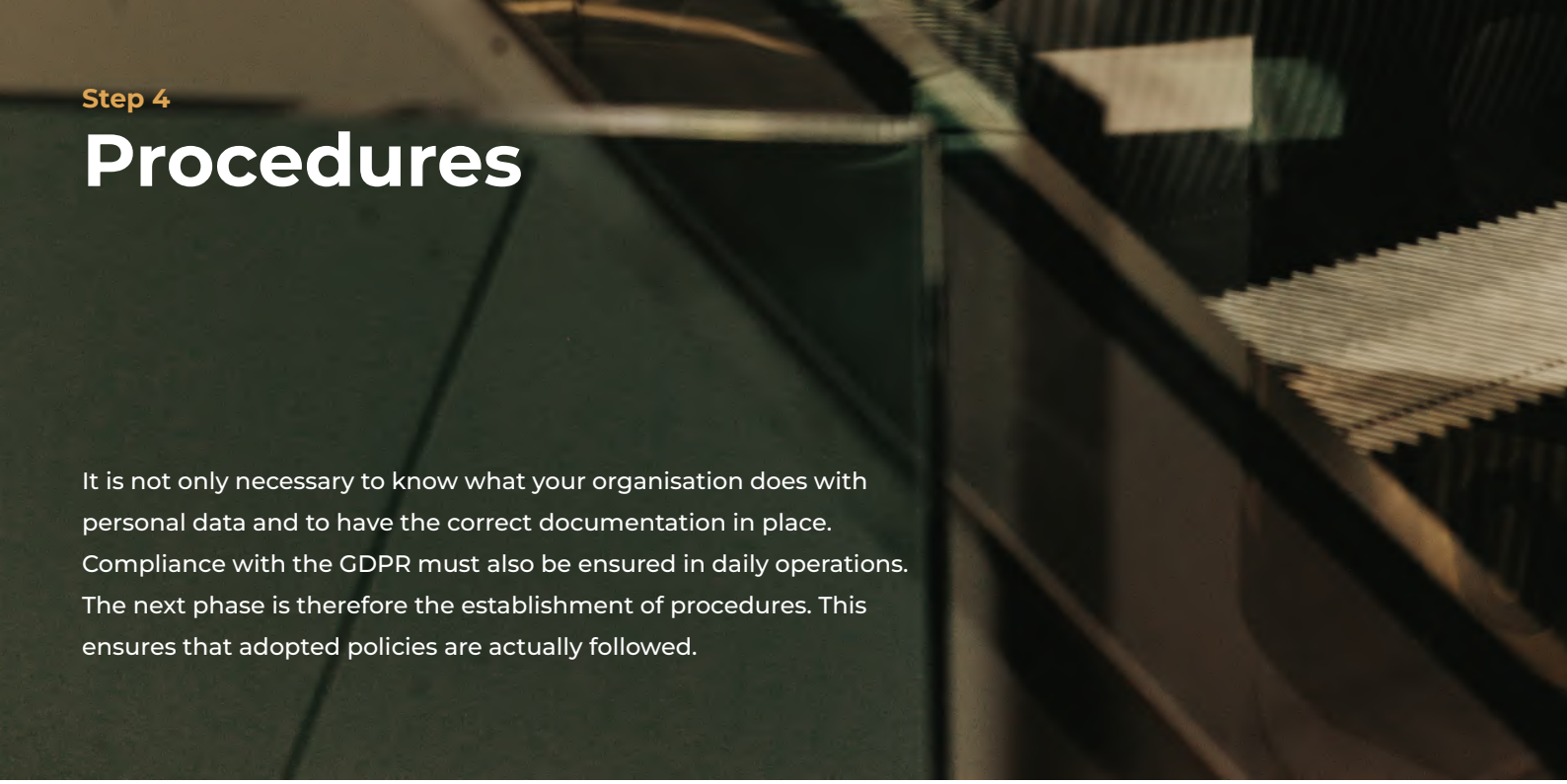
Step 3

Documentation

To comply with the GDPR and to demonstrate that your organisation does so, the following documents must be drawn up:

Document to be prepared	What is it?	Check
Record of processing activities	An overview of all data processing activities within the organisation. A record must be created and maintained for processing activities where your organisation acts as controller and or processor.	◯
Data breach register	An overview of all data breaches that have occurred within your organisation.	◯
Processing agreements and an overview of all concluded and to be concluded processing agreements	Written agreements between the controller and the processor, and between the processor and a sub-processor, regarding the careful handling of personal data. The GDPR prescribes a number of mandatory topics that must be included in a processing agreement.	◯
Data sharing agreement	Written agreements between two joint controllers who exchange data, covering matters such as the handling of data subject rights and the information obligation.	◯
Information security policy	An overview of the appropriate technical and organisational security measures taken and an overview of the security measures that employees must follow, such as a password policy.	◯
Retention policy	A policy document listing the retention periods for the various types of personal data.	◯

Document to be prepared	What is it?	Check
Privacy policy	A policy document describing how employees must handle personal data, such as what to do when a data subject wishes to exercise their rights or what steps to take before procuring a new IT system.	◯
Internal privacy notice	A document explaining which personal data an employer processes about its employees and what happens to those data.	◯
External privacy and cookie notice	A document in which an organisation explains to all external data subjects, such as customers and website visitors, which personal data are processed and for what purposes. Often, this information is combined into a single privacy and cookie notice on the organisation's website.	◯
Data breach incident response plan	A document containing information about data breaches and the internal procedure for handling them. The purpose is to ensure that employees know what a data breach is, that data breaches are reported internally to the correct person and that everyone knows their role in the event of a data breach.	◯



Step 4

Procedures

It is not only necessary to know what your organisation does with personal data and to have the correct documentation in place. Compliance with the GDPR must also be ensured in daily operations. The next phase is therefore the establishment of procedures. This ensures that adopted policies are actually followed.

Procedure	What is it?	Check
Knowledge sharing	It is important that employees know what privacy is, when personal data are processed and why compliance with the GDPR is important. Ensure that knowledge remains up to date and that every new employee is instructed on privacy policies. At the same time, ensure that employees can continue to perform their daily tasks. Excessive or unnecessary interference with daily work for privacy purposes may lead employees to work around the rules.	◯
Engaging third parties	When engaging a third party, such as an IT service provider, it must be assessed whether that party processes personal data for your organisation. If so, written agreements must be concluded regarding the handling of personal data. Internally, it must be clear who is responsible for this and how timely involvement is ensured.	◯
Design of new processing activities	When a new processing activity is initiated, such as sending a newsletter, it must be set up in line with the GDPR. The record of processing activities and the privacy notice must be updated, and where software is involved, it must be designed in accordance with the principles of privacy by design and privacy by default. The privacy officer or DPO must be involved at an early stage.	◯

Procedure	What is it?	Check
Handling data subject rights	Requests from data subjects must be handled within a short timeframe, in principle within one month. An internal procedure must therefore be established that clearly defines who assesses such requests, how requests are forwarded and how they are handled.	◯
Communication regarding data breaches	The data breach incident response plan must also function in practice. It must be clear that the plan exists, that everyone understands when there is a potential data breach and that the relevant staff are easily reachable.	◯
Assessing the need for a DPIA	For high-risk processing activities, a Data Protection Impact Assessment is required. Decide who assesses whether a DPIA must be carried out, who will perform it and ensure that the assessor is informed in a timely manner.	◯
Keeping documentation up to date	An organisation is constantly evolving, which means privacy documentation must be updated regularly. Ensure that responsible persons are designated and that procedures are in place so that these persons, and or the privacy officer or DPO, are informed in time.	◯

Step 5

Awareness and monitoring

Once the organisation has been aligned with the GDPR, it is essential that employees know what to do to ensure continued compliance and, where necessary, adjust their working methods. It is important to disseminate privacy knowledge throughout the organisation and to regularly review and, where necessary, adjust knowledge, documentation, procedures and security measures. The GDPR is not a one-off implementation but an ongoing process that requires continuous maintenance and supplementation. This underscores the importance of appointing internal responsible stakeholders, such as privacy officers, and or a DPO. As soon as your organisation changes or undertakes new activities, the GDPR documentation must be updated or expanded accordingly. In addition, new or changed activities may require specific actions, such as concluding a processing agreement or carrying out a DPIA.

For more information...

Visit **ictrecht.nl/en**,
or contact us via:

Mail contact@ictrecht.nl
Tel 020 663 1941