

TOOLKIT



Checklist record of processing activities



DPO Consultancy
Experts in Data Privacy

Why do you need a record of processing activities?

Before the introduction of the General Data Protection Regulation (GDPR), organizations were obliged to report personal data that they processed to the Dutch Data Protection Authority (AP). This duty to report has lapsed with the introduction of the GDPR. Instead, organizations are required by law to keep a record of processing activities.



A record must be kept if you as an organization employ more than 250 people. An organization with fewer than 250 people must keep a record if one or more of the following situations apply:

- You structurally process personal data. In practice, countless processing of personal data is structural. Consider, for example, a newsletter to customers that you send every quarter or salary payments that you make every month.
- You process personal data that pose a high risk to the rights and freedoms of the persons whose personal data you process. Think of drawing up customer profiles or processing large amounts of data (data from large groups of people or a lot of data from a few people).
- You process sensitive data that falls under the category 'special personal data', such as data about health, criminal data, racial or ethnic origin, political views and beliefs.

What is processing of personal data?

The term 'processing' refers to all kinds of different processing of personal data, whether carried out manually or automatically. In fact, almost everything you do with personal data is seen as processing. Some examples:

- Personnel and salary administration
- Consulting a file with contact details of persons
- Sending a newsletter or other marketing-related e-mails
- Shredding documents with personal data
- Placing photos of persons on a website
- Saving of IP addresses

“It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you’ll do things differently.” Warren Buffett





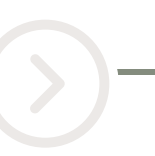
What is a record of processing activities?

A record of processing activities is a document in which all processing activities carried out by an organization are kept. This gives you insight into the processing within your organization and you can comply with the accountability obligation of the GDPR. If the Dutch Data Protection Authority asks your organization for a record of processing activities, you must be able to demonstrate which personal data you process and why.

How do you draw up a record of processing activities




The record of processing activities is a living document that you as an organization constantly supplement with new processing activities and update when things change during a processing. Repeated and one-time processing is included in the document. For a newsletter that you send quarterly or for the payroll, you create a processing once. You do not have to record a processing for every newsletter. For activities that only take place once, you have to create a new processing every time.






As an organization you can decide for yourself how to compile a record of processing activities. Many organizations choose to keep the record in Excel. This is a great option for a small number of processes, but it is quite prone to error and laborious if you record numerous processes. That is why various (online) tools are available that offer the possibility to compile and supplement the registry in a safe, user-friendly and fast way.



Checklist for the record of processing activities

With this checklist we explain which matters you must include in a record of processing activities according to the GDPR. In addition, we also provide an explanation for each point and explain what you should take into account.

	Legal obligation	Explanation
	The name and contact details of the controller or his representative, if the controller is located outside the EU.	In most cases, you as an organization are responsible yourself. If your organization comes from outside the EU, but processes data from people in the EU, you are obliged to appoint a Data Protection Representative (DPR). This is your representative within the EU and the point of contact for the AP and those involved if they have questions about the processing of personal data.
	For what purposes are the data processed?	<p>What do you need this data for and how do you process it? For example for the recruitment and selection of personnel, the delivery of products or direct marketing. You always need a clear and deliberate goal. If you do not have this, you may not process personal data.</p> <p>In addition, it is advisable to also state the basis for each of your processing activities. You are not required to do this, but it can help you meet your accountability obligations at a later stage.</p>
	Which category of personal data do you process?	You do not have to describe exactly which data you will process. The category is sufficient, as long as it is clear what it is about. For example, make a distinction between name and address details, contact details, payment details, medical details, IP addresses, credit card details and login details.

	Legal obligation	Explanation
	From which category of data subjects do you process data?	You describe the categories of persons whose data you process. For example, customers, website visitors, employees, patients, clients, etc. Keep in mind that sometimes you process data from several categories at the same time. For example with a newsletter. You may send them to customers and website visitors.
	To which category of recipient are the data provided?	This category does not always apply. Recipients are the parties to whom you provide the personal data. For example, as a municipality you are legally obliged to provide information to the tax authorities. For an organization, this may, for example, concern the provision of personal data to an accountant, insurer or the tax authorities.
	Do you share data with a country or international organization outside the EU?	This applies if you use services located outside the EU. A good example of this is the storage of personal data in the cloud with a service provider from the United States. If you do so, you are obliged to indicate this in the record of processing activities. Usually you enter the party from which you are purchasing the service here. It is also advisable to explain under which right you share data outside the EU.
	How long do you keep personal data and when will it be deleted?	You may be required by law to keep personal data for a number of years and / or that you keep data longer, because, for example, you give customers a ten-year guarantee on certain products and therefore see the need to keep personal data. You can record such retention periods here.
	How are the personal data secured?	Here you provide a general description of the technical and organizational measures you have taken to protect the personal data you process. Examples of technical measures include encryption, logical access control and pseudonymization. Among the organizational measures you include a confidentiality statement and the processor agreement.



Getting started

By compiling a record of processing activities, you always have control over which personal data you process within your organization, in which systems they are located and for what purposes you collect them. This way it is always clear what you do with personal data and what you use it for. In the event of a calamity, it is therefore easy to find out which data may be involved in this calamity.

**Are you not quite sure, or do you have
additional questions about specific topics?
Please contact us via info@dpoconsultancy.nl
or **+31 85 0711080****

Australiëlaan 12a
5232 BB 's-Hertogenbosch
the Netherlands

Rue du Congres 35
1000 Brussel
Belgium

1 Lyric Square
London, W6 0NB
England

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

