MANUAL

EASYDPIA®

Inhoud

Manual

1. Starting with EasyDPIA®

Congratulations. By creating an account on EasyDPIA® you have taken the first step to easily perform and manage DPIA's. In this manual we will guide you through the software step by step.

A key obligation of the General Data Protection Regulation (GDPR) is that organisations must be able to demonstrate that their data processing complies with the rules of the GDPR. An important tool from the GDPR is the Data Protection Impact Assessment (DPIA). The way in which a DPIA is performed is free of form and there are various methods to make a DPIA report. The methodology in EasyDPIA® is based on the models in the DPIA Handbook. These models have been developed on the basis of various DPIA standards (including the Dutch DPIA Government model) and the DPIA models of the CNIL (French regulator) and the ICO (English regulator). This ensures that the DPIA meets the requirements of the GDPR.

2. Profile creation

On the left-hand side of the home screen (or in the top right-hand corner under your photo or initials), you can find and change your personal details under 'Your Profile'. On this page you can further personalise your profile by adding your photograph and the logo of your organisation. This logo will appear on the cover page of the reports that you will make with EasyDPIA®. This page also allows you to change your password, display two-factor authentication recovery codes (which you can then copy and save elsewhere) and manage your browser sessions.

> **Please note:** when the account is deleted, all linked files and data are also permanently deleted.
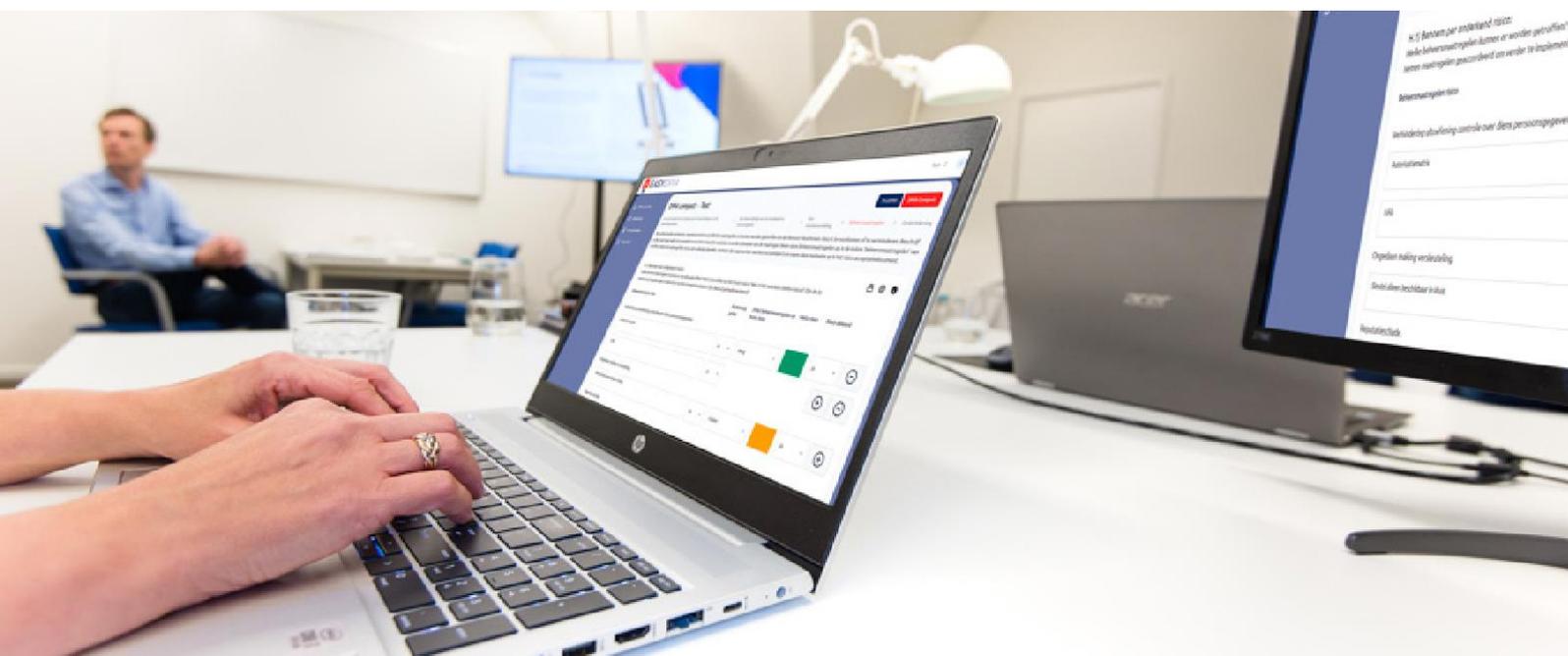
3. Create new DPIA or participate in DPIA's

In the home screen (click on 'DPIA overview' or on the EasyDPIA logo) you can see which DPIA(s) you are involved in.
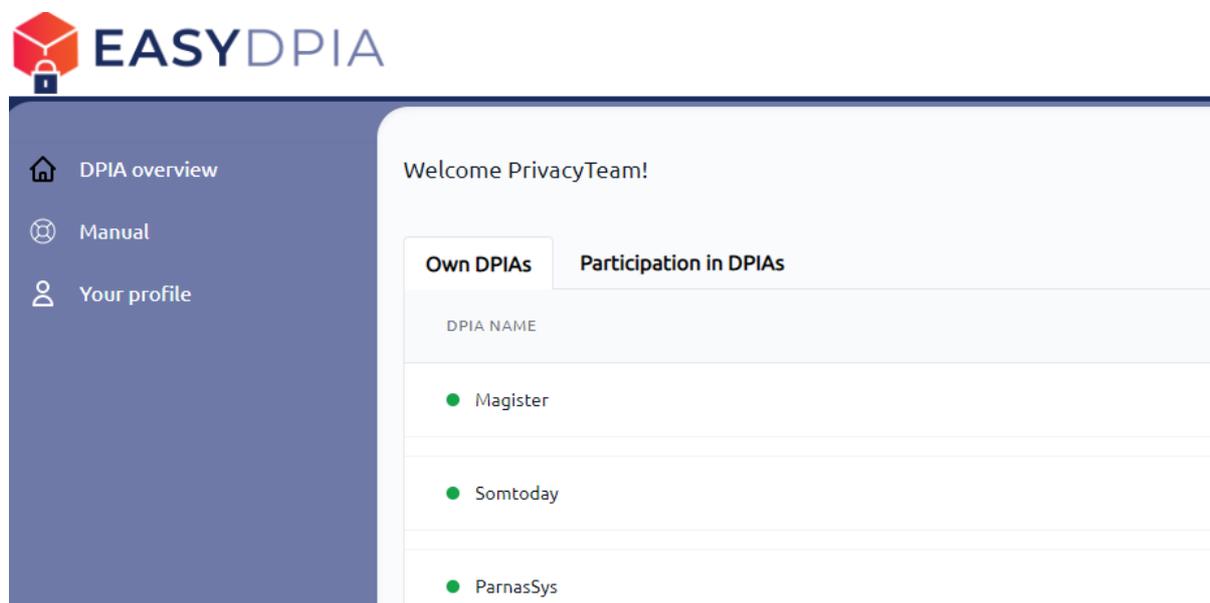
You will see one or two tabs. One (Own DPIAs) containing the DPIA's that you have created yourself and / or a second (Participation in DPIA's) containing DPIAs created by others in which you participate. If you created an account after receiving an invitation to participate in a DPIA, you will find the DPIA for which you were invited here.

In the top right-hand corner of your home screen you will see a blue button with the words 'Create new DPIA'. Use this button if you want to create a DPIA yourself. You can enter the name of the new DPIA and maybe choose an existing DPIA from the library.

> **Please note:** if you choose an existing DPIA from the library, it is already largely filled in and you only need to tailor and complete it for your organisation. PrivacyTeam is continuously working on the expansion of the DPIA library in EasyDPIA®.

If you create a DPIA yourself, you always start with the Pre-DPIA (see also under 5.). As soon as you have completed this and chosen to make a compact or comprehensive DPIA, the texts you entered in the Pre-DPIA are automatically included in the compact or comprehensive DPIA.

You also enter the date when the DPIA must be started or when it must be revised. In this way, you can create a planning for the implementation or revision of your DPIA's. This supports the PDCA cycle to maintain and periodically update DPIA's.

Once you have created a DPIA, you continue by putting together the team with which you want to work on the DPIA. You can invite people to participate in the DPIA and you can choose from various roles. See the chapter about the team composition and the various roles.

> **Please note:** if you are invited to participate in a DPIA, you can also create your own DPIA. You can start by making a Pre-DPIA without any costs. However, if you want to carry out more Pre-DPIA's or if you want to make a complete DPIA (model compact or comprehensive), you will have to take out a subscription for EasyDPIA® yourself.

The person who is invited by you to participate in a DPIA can create an account him/herself or - if he/she already has an account - he will see this DPIA appear under Participation in DPIA's in the home screen.

After you have added people to your team, click on the button [ready with selecting the team] and you can start working on the DPIA.

4. Team selection and roles

In EasyDPIA® you can work on a DPIA with a team. For this purpose, the system has several roles that you can choose when putting together your DPIA team.

The roles:

<u>Administrator</u>: the administrator of the licence. He can start new DPIA's and also has the role of DPIA owner on all DPIA's.

<u>DPIA owner</u>: the owner of a DPIA. He is given the rights to a specific DPIA. The DPIA owner can compose the DPIA team. The DPIA owner can change, duplicate, freeze and delete the DPIA, ask questions to team members or external parties, can download and print the reports and can add documents. The DPIA owner can be someone other than the Administrator.

DPIA participant: the participant in a DPIA can fill in the DPIA, ask questions to team members or external parties, can download and print the reports and can add documents.

Data Protection Officer: the DPO can view the DPIA, can make comments, can mention the DPIA advice in the DPIA, can download and print the reports and can attach documents.

Data Controller: the data controller can view the DPIA, make comments, download and print the reports and can add documents and formally adopt the DPIA (after which the DPIA owner can freeze the DPIA).

All the people who are part of the DPIA team (with their roles) can be found in the DPIA management (top right) under DPIA settings.
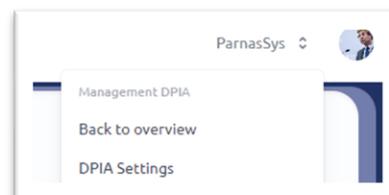
5. The Pre-DPIA

In EasyDPIA®, every DPIA process always starts by performing a Pre-DPIA. By means of the Pre-DPIA it becomes clear whether the execution of a DPIA is compulsory. When there is no need to carry out a DPIA, the Pre-DPIA report remains available in EasyDPIA®.

If a DPIA must be carried out, the content of the completed Pre-DPIA is reflected in the model that is compiled for the DPIA (model compact or comprehensive).

> **Please note:** if you use a DPIA from the library as a basis, it is already clear that a DPIA must be performed and you start directly in the compact or comprehensive model.

6. Record of processing activities

The data entered during the Pre-DPIA also become available immediately as a 'record of processing activities' report and can be used to complete your existing record of processing activities. If you have carried out a Pre-DPIA of all processing activities, then you have a complete record of processing activities for the organisation.

7. The DPIA

If the Pre-DPIA reveals that a full DPIA is required, you can use a simple decision aid to determine whether you should carry out a DPIA using the compact model or using the comprehensive model.

The content of the completed Pre-DPIA is automatically transferred to the template for the full DPIA.

After filling in the systematic description of the processing activity and the processing purposes, and the assessment of the necessity and proportionality of said processing activity, you can carry out an assessment of the risks associated with the processing (both for the data subjects and the organisation). You can then list the control measures that have already been taken or will be taken as an outcome of the DPIA.

G.1) Describe and determine the (gross) risks to stakeholders.
Gross risk refers to the risk to individuals or organization without (additional) measures being taken.

1 Discrimination against an individual. ⌄	▤	Almost certainly in the coming year ⌄	€ 4.000.000
2 Undoing encryption ⌄	▤	More than once in coming year ⌄	€ 500.000

Please note: You can choose risks in the select box or add risks yourself by clicking on the icon on the right. If you click the icon a second time, the select box with choices will return.

After you have entered a risk and determined the probability of chance and the impact, EasyDPIA® classifies the risk (gross risk). The colour of the risk indicates the level of the risk. On the next page you can indicate which control measures should be taken to mitigate the risk.

H.1) Name per risk identified.
What control measures can be taken? What is the effect on gross risk? What is the residual risk (net risk)? Have the measures to be taken been approved for further implementation? Have they already been implemented?

Risk control measures	Already present yes/no	Effect of control measures on gross risk	Net risk
Discrimination against an individual.			
Test	Yes ⌄	Medium ⌄	
Undoing encryption			
Test	No ⌄	Low ⌄	

For each risk, you can indicate one or more (with the plus sign) control measures. Indicate whether these are already in place or not (if they are not yet in place, they will appear on the action list in the report) and what the mitigating effect of the control measure is on the gross risk (low/medium/high).

The net risk (the gross risk minus the total effect of the control measures) is then shown and you can indicate whether the risk has been sufficiently mitigated and is therefore deemed to be acceptable. The aim here is to ensure that there are no high residual risks.

Should the risk still be high or not acceptable and should no additional control measures be possible, you can - prior to the processing - consult the relevant Data Authority for advice.

> **Please note:** if you have entered several control measures (present or not) for a risk, the whole of the control measures will determine the effect on the gross risk.

8. Calling for help

You can ask for help with every question in EasyDPIA®.
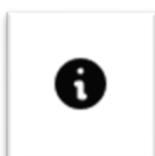
Below the i you can find information that will help you answer the question.

If you click on a question, this symbol will appear. You can use this to ask a question to a team member or to an external party (e.g. a processor). He or she can answer directly in the screen.

> **Please note:** When making a comment, please describe clearly what you are doing and what your request is. The question appears as you see it on your screen and may need some context.

When the help question has been answered, you will see this symbol appear. If you click on this symbol, the answer given will be copied directly into the question. If you click on this symbol again, the answer that was given previously will be returned. By the way, version control also remains available (see below).

If a teammate asks you for help, you will see a green question appear at the top of your screen. It looks like this:
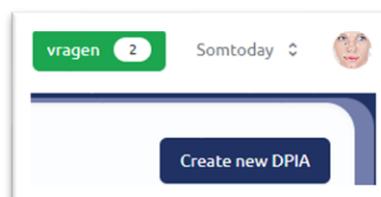
You can answer the question on the page, after which the block will disappear.

In the event that the Data Protection Officer or the Controller makes a comment, a 'bell symbol' will appear on the screen to draw your attention to it.

9. Versioning

 If this symbol appears above a question, it means that several versions of the given answers are available. You can choose from the previously given answers and possibly replace an earlier answer.

Since several people can work on the same DPIA, the question is blocked for other users if someone is working on it. The name of the person working on the question will appear under the question.
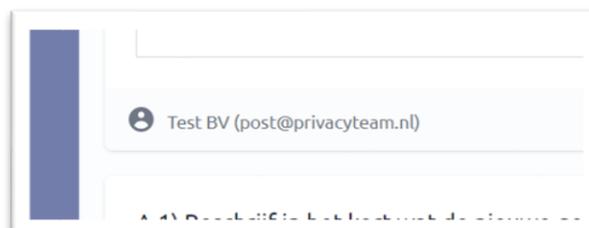
This ensures that no two people can work on the question at the same time. As soon as someone else starts working on the question, it is blocked for that person and their name appears under the question. Version control then keeps track of the answers given previously (by others) and these can also be placed back if required.

10. Comments DPO or controller

If you have also given someone in the team the role of DPO or data controller, this person can comment on the questions and give his advice on the DPIA that has been performed. The owner of the DPIA can also give his reaction to the comments of the DPO. This information remains available in the digital version but will not be included in the report. The data controller can adopt the DPIA (and thereafter the owner can freeze the DPIA, after which it can no longer be changed). The DPIA is provided with a 'deadline' date, after which the DPIA must be updated. With this, the PDCA cycle is automatically implemented.

11. Modify, duplicate, freeze and delete

If, as a DPIA owner, you click on the right-hand side of the DPIA overview page on the 'three dots' symbol associated with a DPIA, you will see a pop-up.

Here you can change the DPIA name and team composition, you can duplicate the DPIA without losing the previous information (e.g. for review), or you can freeze the DPIA so that it cannot be worked on again (after completion).

You can also remove the entire DPIA.
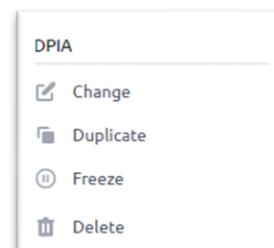
Please note: once a DPIA is deleted, it cannot be retrieved

12. Reports and uploads

If you click on the 'three dots' symbol on the right of your screen, you will see a pop up.

You can choose different reports here. The register of processing activities is an overview of all the information that must be included in a register of processing activities according to the GDPR (if completed). In this way, you can easily compile your own register.
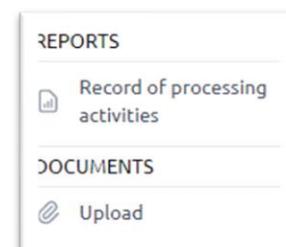
In addition, you can make a report of the Pre-DPIA or the complete DPIA (Compact or Comprehensive). The reports are available in PDF and Word.

You can also add documents to the DPIA when uploading, such as a processing agreement, advice from the DPO etc.

13. Signing

On the sign page you can indicate (among other things) who collaborated on the DPIA, who approved the control measures to be taken, etc. You can also enter the date when the DPIA should be revised. In this way, you can create a planning for the implementation or revision of your DPIA's. This supports the PDCA cycle to maintain and periodically update DPIAs. You can also indicate who, when, is expected to review the DPIA. This person will receive a message by e-mail with the possibility to record this moment in the (Outlook) agenda.

> **Tip: click on import to add the appointment to your existing calendar.**.
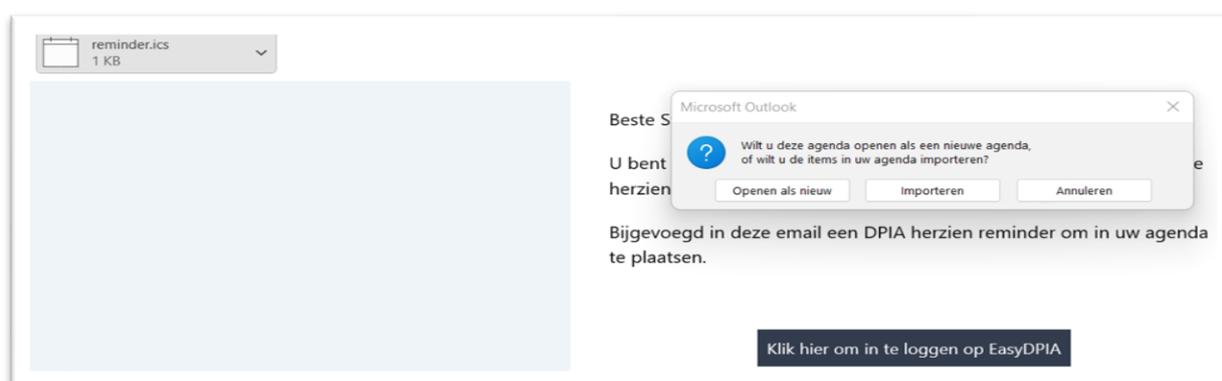
14.   Data Privacy & Security

PrivacyTeam considers the proper handling of personal data and the proper protection of personal and other data, including confidential business information regarding risks and the management measures taken, as very important. EasyDPIA® is secured according to the current 'state of the art' and an comprehensive Data Privacy & Protection Policy has been drawn up. This can be found together with the terms of use, the abridged processor's agreement and the cookie statement in the information about your subscription (top right under account management) or at www.privacyteam.nl.

15.   General

EasyDPIA® is a product of PrivacyTeam B.V. EasyDPIA® was developed by experienced DPIA specialists and enables you to easily conduct your own DPIA's and create and manage DPIA reports. In case you have suggestions for the improvement or further development of EasyDPIA®, please send an e-mail to post@privacyteam.nl or contact us (privacyteam.nl).

PrivacyTeam thanks you for using EasyDPIA® as your easy tool for performing DPIA's