Terms of Use

(INCLUDING DATA PRIVACY & SECURITY POLICY / DATA PROCESSING AGREEMENT AND COOKIESTATEMENT)

EASYDPIA®

Terms of Use

Agreement

Prior to the provision of the Programme (EasyDPIA®), you as the Client have expressly agreed to these Terms of Use as well as the Data Privacy & Security Policy contained therein, which you have had the opportunity to review prior to giving your consent. You have also accepted the General Terms and Conditions as well as the extended Processing Agreement with the commissioning of EasyDPIA®.

Definitions

The Programme:

The EasyDPIA® programme.

PrivacyTeam:

PrivacyTeam B.V., the creator of the Programme.

Client:

The (legal) person who has paid the invoice for the licence(s) to use the Programme to PrivacyTeam. This is also the Controller.

User:

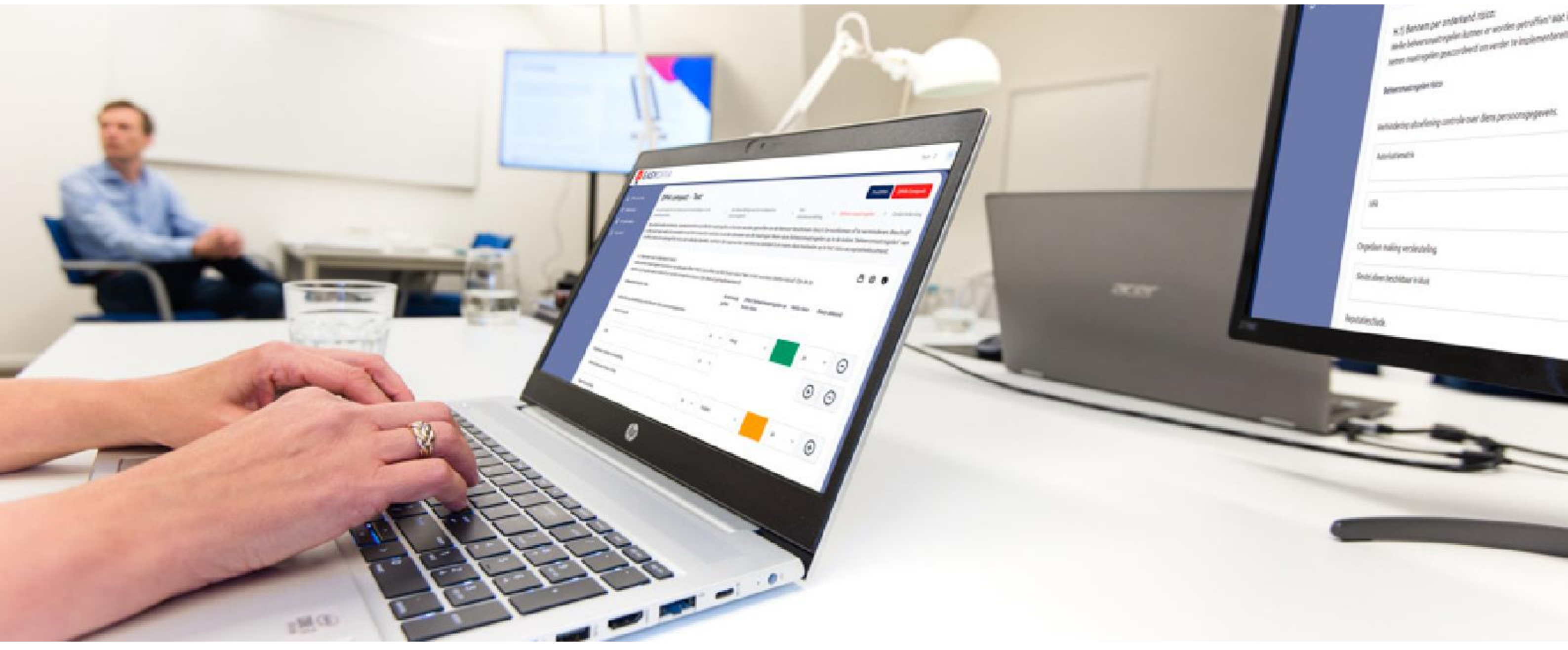
The person who uses the Programme by logging into it. At first login, the User's email address is verified. After initial login, the User is responsible for creating his/her own password and setting up two-factor authentication on the access.

Customer:

The customer is understood to mean both Client and User, separately but also together.

Terms of Use:

These terms of use as they apply from time to time, including the Data Privacy and Security Policy contained therein, as well as the abbreviated Data Processing Agreement and Cookiestatement.



Starting point

The Customer can use the Programme via the Internet. Customer may not allow others to access the Programme other than in the manner provided in the Programme. PrivacyTeam grants Customer a non-exclusive, non transferable license to use the Programme, solely for the contracted (legal) person.

1. Operation and maintenance

Customer agrees to the operation of the Program 'as is' at the time of provision by PrivacyTeam. PrivacyTeam may always modify the Programme. This will normally be done to improve the program but PrivacyTeam is not obliged to do so. If Customer wishes to change the way the Program works, Customer can communicate this to PrivacyTeam. PrivacyTeam will then review the matter and determine whether it can be amended, and whether this can be done free of charge or whether an invoice is generated

2. Rights

Customer explicitly does not own any rights to the source code of the Programme, nor to the content of the information, models and documents made available through the Programme. The intellectual property rights relating to the Programme and the information, models and documents are vested exclusively in PrivacyTeam. Customer may use the generic DPIAs to create his 'own' - organisation specific - DPIA. Customer may not make the information available to third parties in any way. Copying or reproducing the software to another server or location (regardless of the purpose, including further reproduction or redistribution), or disclosing the information made available is expressly prohibited, unless prior written consent of PrivacyTeam is obtained.

3. Database

PrivacyTeam is not responsible for the database edited by the Customer. PrivacyTeam cannot be held responsible for the content, nor for the condition of the database.

4. Damages

PrivacyTeam cannot be held liable and does not accept any liability concerning the use and/or consequences of the use of the Programme and the information made available, including documents (including generic DPIA's). Damage caused by the use of the Programme or the information made available by it, of whatever nature, irrespective of how it is caused, as well as consequential damages can never be recovered from PrivacyTeam.

5. Problems

The Programme is used 'as is'. If the User experiences any problems, the User can contact the Client. The Client can contact PrivacyTeam. PrivacyTeam will make every effort to provide a solution.

6. Security

PrivacyTeam provides and will maintain adequate technical, physical and organisational measures to protect User's data in the Programme against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access.

The combination of e-mail address and password is linked to a natural person (User). The User is responsible for keeping the login details, including the password, secret. PrivacyTeam will never be liable for any damage, including consequential damage, caused by the use of the account or password by unauthorised persons.

For more information, see the privacy statement.

7. Access to the Programme

The licence for the use of the Programme and the information made available with it is valid for the period for which it has been paid.

8. File size and storage space

A 'Fair Use Policy' (FUP) is used as standard. This means that the Customer receives an amount of storage space that can reasonably be expected for the relevant software licence.

9. Webserver availability

The web servers for the Programme have been placed by PrivacyTeam with a company specialised in this field in the Netherlands. These web servers guarantee maximum availability to PrivacyTeam. However: PrivacyTeam cannot be held responsible and does not accept any liability if a webserver might be temporarily unavailable.

10. EasyDPIA®

The information, models and documents (including: generic DPIAs) provided by PrivacyTeam to the Client through the Programme, have been drawn up according to the latest insights or are provided by third parties (for generic DPIA's). However, PrivacyTeam cannot guarantee that by using the information all legal requirements and regulations are fully met, nor can PrivacyTeam guarantee that a DPIA will always be up to date in the future.

Customer remains responsible and liable for, among other things: the management and operation of its company/organisation, the adequate performing of the DPIA, with which it intends to comply and demonstrate compliance with laws and regulations, and the associated management measures and actions / controls within Customer's operational and security processes and their maintenance, the legal obligations and its own business matters.

11. Special personal data

The Programme is not designed to store special personal data. Therefore, in the context of the GDPR, it is not allowed to process special personal data with the Programme

12. Continuation and termination

If the Customer does not terminate the agreement, the licence for the Programme will always be renewed automatically for the same period. Customer can terminate via the button 'subscription' in the Programme. Customer may also terminate by e-mail or telephone. Notice of termination must be received by PrivacyTeam at least 1 month before the expiry of the licence period. The license period is mentioned on the invoice.

Price increases are always communicated to the Customer in good time, so that the Customer can cancel if he does not agree with the price change.

The contact details are:

PrivacyTeam B.V.

Amersfoortseweg 38
3951 LC Maarn, The Netherlands
Telephone: +31 (0)33 - 200 30 83
E-mail: post@privacyteam.nl

13. Deletion of data

After termination, the Customer's data will be retained for 30 days. After 30 days PrivacyTeam will delete all data of the Customer from its servers.

14. General terms and conditions

To all deliveries of PrivacyTeam general terms and conditions apply. These are accepted by the customer upon entering into the licence. They can also be found on the website of PrivacyTeam (www.privacyteam.nl).

15. Modification of Terms of Use

We may update the Terms of Use from time to time. However, we will never make any changes that would have a negative effect without prior notice to our customers.

We will inform our Customers of any changes by updating and re-issuing these Terms of Use via EasyDPIA®. We recommend reviewing them regularly so that the Customer is aware of these changes.

Data Privacy & Security Policy

1. Data privacy & security policy

The information we collect is valuable to our Customer, as it relates to data processing and the risks associated with it. This business information is often confidential and must be protected properly. We also process personal data. This personal data is 'normal' personal data, such as name and e-mail address. No sensitive or special personal data are processed. PrivacyTeam makes every effort to ensure that the information we collect is stored securely and used safely and responsibly.

We process personal data only on behalf of the Client and/or User.

This policy describes the information we collect, where it is stored, how it is used and how it is secured.

> This declaration applies to EasyDPIA® and the information processed by us.

2. Data in EasyDPIA®

EasyDPIA® is a SaaS solution with which DPIAs can be created and managed. Besides the data of the customer, personal data of the participants in a DPIA are recorded in EasyDPIA®. At the choice of the participant, he or she also adds a photo of him or herself. This is however entirely voluntary. Additionally, in EasyDPIA® the data concerning a DPIA are registered, including the risks connected with the processing activity and the control measures taken as a result of this.

3. What information do we record?

What information?	Nature of the information	Application
User name	Personal data	EasyDPIA®
User E-mailadres	Personal data	EasyDPIA® Postmark
IP-address	Personal data	EasyDPIA®
Photo user	Personal data	EasyDPIA®
Company name	Business information	EasyDPIA®
Company data	Business information (data relating to business operations connected with the) processing of personal data.)	EasyDPIA®
Payment details	Business (financial) information	Stripe

4. Where is the information stored and who has access to it?

We record the information we receive in a number of applications:

Application	Description	Hosting	Accessible to
EasyDPIA®	SaaS application	LinQhost (NL)	- employees MaxiCMS - employees LinQhost - PrivacyTeam staff
Stripe	SaaS application for payment services	AWS (US)	- employees MaxiCMS - PrivacyTeam staff
Postmark	Mail service	AWS (US)	- employees MaxiCMS - PrivacyTeam staff

PrivacyTeam has made arrangements with the suppliers of the applications to secure the information (including personal data) in an adequate manner. If data are stored outside Europe, agreements have been made with the suppliers via Standard Contractual Clauses (SCC).

Through Postmark and Stripe, personal data is processed in the United States. Since the Schrems II ruling of July 2020 of the European Court of Justice, the US is considered 'not adequate' and it is not allowed to have personal data processed in the United States without an additional risk assessment.

In addition to the SCC, a Data Transfer Impact Assessment (DTIA) was carried out by PrivacyTeam. Because there is only data processing of a business e-mail address and names, and therefore no sensitive and/or special personal data are processed, there is no high privacy risk. Therefore, the data processing as mentioned above is permitted. We can make the results of the DTIA available upon request.

Description of measures to ensure that only authorised PrivacyTeam personnel have access to the processing of Personal Data	
Employees and data:	**Acts:**
Employees have access to the licence information. They can see, among other things, which licence has been purchased and the corresponding contract period.	Administrative actions in the context of licensing. End user support.
Employees have access to customer information.	End user support.
Employees have access to payment information. They can see contact details and payment information, among other things.	Administrative actions within the framework of the licences. End user support..
IT data managers have access to the databases.	The actions of IT database administrators are aimed at continuity and optimisation of ICT systems.

This always concerns a limited number of employees who have access to the information ('need to know' basis). The employees who have access to the information have all signed a confidentiality agreement.

5. How long is the information stored?

Type	Information	Actions	Storage period
EasyDPIA®	User data	Delete account	Directly removed
	Customer data (including DPIA's)	Termination of licence	30 days

Stripe	Payment details	Termination of licence	7 years
Postmark	E-mails	-	30 days

6. With whom do we share the information?

The information will not be shared with other third parties other than on the basis of what is stated in these terms and conditions, or on the basis of a statutory provision or a judicial decision, or when PrivacyTeam is required to disclose confidential information to a third party designated by law or by the competent court, and PrivacyTeam cannot in this matter invoke a legal right to refuse to give evidence or a right to refuse to give evidence acknowledged or allowed by the competent court.

7. How is the information secured?

PrivacyTeam will always and continuously make efforts to take adequate technical and organisational measures to protect the information against loss or against unauthorised access, impairment or modification.

Encryption	All network connections to the web server are secured with TLS encryption. The certificates are managed externally by LinQhost. They purchase our certificate from Sectigo. We do not have access to the certificate file ourselves.
	The data on the server is encrypted with AES-256-CBC.
	The key is stored encrypted outside the software (double key encryption).
	Passwords are stored encrypted with Argon2id.
Identity and access management	The user is required to set up two-factor authentication.
	After five attempts to log in with an incorrect password, an account is locked for an increasingly long period at each subsequent attempt.
	Accounts are associated with individuals, there are no shared system accounts.
Server security and hardening	The web server is protected from network-based attacks from the Internet by firewalls.
	The entire online platform is provided with current security updates.
	A SLA is in place for creation of backups and backups are made very regularly.

Web application security	The web application is protected against different types of attacks, such as XSS, SQLi, RFI, LFI, User Agent and many more. The firewall also blocks repeated attacks and sends notifications when an attack is detected. Moreover, it will log failed logins and block the IP address after a number of attempts.
Hosting	Our services (database, API, etc.) are hosted in an ISO 27001-certified data centre.
Logging and monitoring	The level of detail in logging is sufficient to be used in attacks to find out the attacker's modus operandi and network identity.
	Critical system functions are monitored and disruptions are reported to system administrators and followed up by means of a "learning" monitoring and alert system.
Secure management	Remote access to servers is secured in multiple ways.
	An adequate back-up plan and restore plan have been worked out.
Testing	PrivacyTeam regularly tests the security of the Software.
Patches	PrivacyTeam ensures that security patches are installed as soon as they become available.
Policy	PrivacyTeam has an Information Security Policy.
Employees	Confidentiality agreements and information security agreements are made with employees.
	PrivacyTeam promotes information security awareness, education and training.
	Employees have no access to more data than is strictly necessary for their jobs, based on an authorisation system.

8. How do we deal with the rights of data subjects?

In the situation that PrivacyTeam is a processor of personal data, the following applies: if a data subject directs a request to PrivacyTeam to exercise his/her statutory rights, PrivacyTeam is not authorised to deal directly with the data subject's request. PrivacyTeam will only deal with the requests coming from the Customer.

In the situation where PrivacyTeam is a controller of personal data, the following applies: privacy law gives everyone whose personal data is processed a number of rights to ensure that the processing of personal data is done in a fair and transparent manner.

You have the following rights:
- get an explanation of what personal data we process;
- access to the exact personal data we process;
- having errors corrected;
- the deletion of (outdated) personal data;
- withdrawal of your consent;
- object to a particular use.

You can exercise your right by submitting a written request to us. It is important that you can identify yourself and prove that the request actually concerns your own personal data. It is not permitted to request the personal data of others. We will respond to your request within one month. In the case of many or complex requests, we may extend this period by up to two months. In the case of extensive requests, we may charge you a fee.

9. What do we do in case of an incident?

PrivacyTeam will inform the customer of security breaches according to Article 33 of the GDPR without unreasonable delay.

PrivacyTeam shares at least the following information when an incident or data breach occurs:

- the nature of the personal data breach, where possible indicating the categories of data subjects and personal data records concerned and, approximately, the number of data subjects and personal data records concerned;
- the name and contact details of the data protection officer or other contact point where further information can be obtained;
- the likely consequences of the personal data breach;
- the measures taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

For a detailed description of how PrivacyTeam, as processor, processes personal data, please refer to the Data Processing Agreement, which is included in the General Terms and Conditions.

Cookiestatement

EasyDPIA® is a web application and not a website. Only the login and register page use a web address to enable access to the application.

To make use of EasyDPIA®, only necessary cookies are used by PrivacyTeam B.V.. No prior consent of the User is required for this.

The following Cookies are used:
A session cookie and an XSRF-Token.

- A session cookie is placed to allow EasyDPIA® to function properly (functional cookie). It stores data temporarily (during the session).

- An XSRF-Token is a security measure and serves to prevent so-called 'cross-injections'. This is also a necessary cookie to ensure secure use of EasyDPIA®.

EasyDPIA® does not use analytical or tracking cookies.