GEBRUIKSVOORWAARDEN

(INCLUSIEF DATA PRIVACY & SECURITY POLICY / VERKORTE VERWERKERSOVEREENKOMST EN COOKIEVERKLARING)

EASYDPIA®

Gebruiksvoorwaarden

Akkoord

Vóór beschikbaarstelling vanuit PrivacyTeam van het Programma (EasyDPIA®) bent u als Klant uitdrukkelijk akkoord gegaan met deze Gebruiksvoorwaarden alsmede de hierin opgenomen Data Privacy & Security Policy, welke u voorafgaand aan het geven van een akkoord heeft kunnen bestuderen. Tevens heeft u de Algemene Voorwaarden alsmede de Verwerkersovereenkomst met de ingebruikname van EasyDPIA® aanvaard.

Begripsomschrijvingen

Het Programma:
Het programma EasyDPIA®.

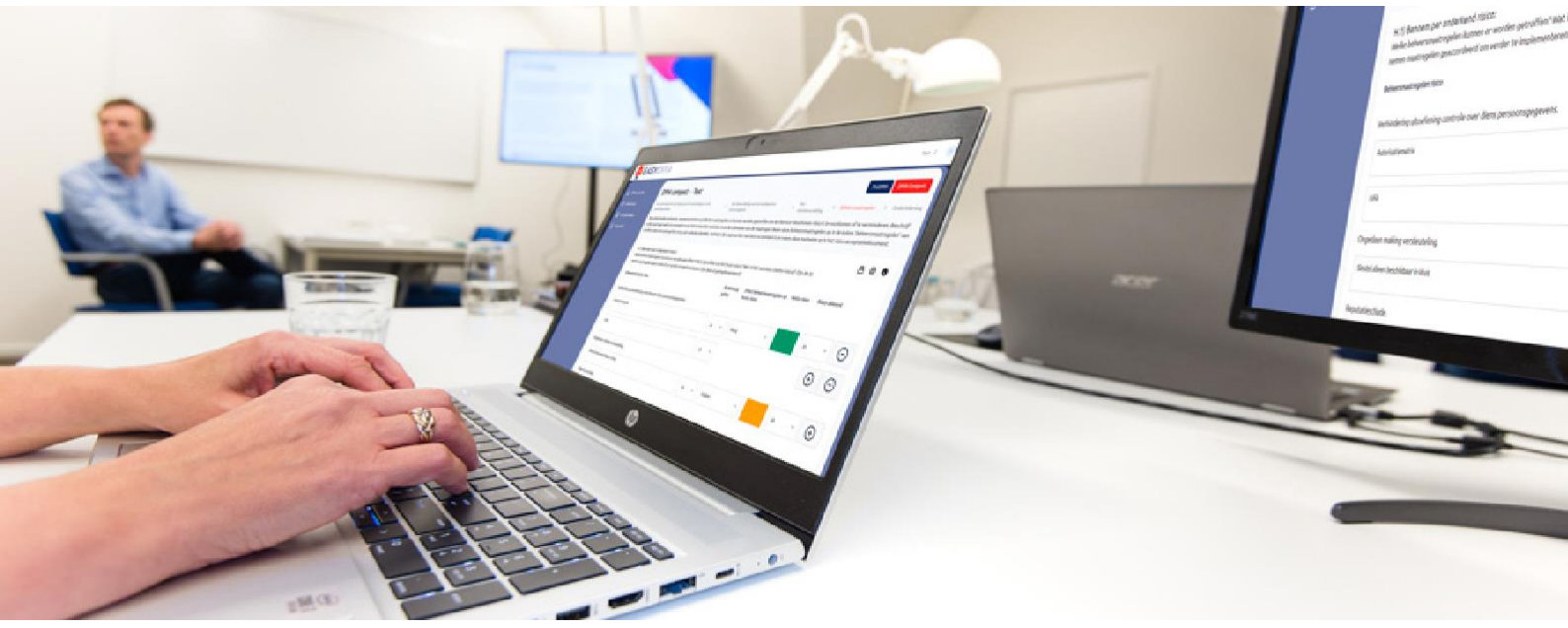
PrivacyTeam:
PrivacyTeam B.V., de makers van het Programma.

Afnemer:
De (rechts)persoon die de factuur voor de gebruikslicentie(s) van het Programma aan PrivacyTeam heeft betaald. Dit is tevens de Verwerkingsverantwoordelijke.

Gebruiker:
Degene die het Programma gebruikt door erop in te loggen. Bij de eerste inlog wordt het e-mailadres van de Gebruiker geverifieerd. Na eerste inlog is de Gebruiker zelf verantwoordelijk voor een eigen wachtwoord en het instellen van tweefactor-authenticatie op de toegang.

Klant:
Met de klant wordt zowel Afnemer als Gebruiker bedoeld, afzonderlijk maar ook beiden tezamen.

Gebruiksvoorwaarden:
Deze voorwaarden zoals ze van tijd tot tijd gelden, inclusief de daarin opgenomen Data Privacy en Security Policy, alsmede de (verkorte) Verwerkersovereenkomst en Cookieverklaring.



Uitgangspunt

Via het Internet kan Klant het Programma gebruiken. Klant mag anderen geen toegang verschaffen tot het Programma anders dan de wijze waarop in het Programma is voorzien. PrivacyTeam verleent Klant een niet-exclusieve, niet overdraagbare gebruikslicentie op het gebruik van het Programma, uitsluitend voor de gecontracteerde (rechts)persoon.

1. Werking en onderhoud

Klant gaat akkoord met de werking van het Programma ‘zoals het is’ op het moment van beschikbaar stellen door PrivacyTeam. PrivacyTeam mag het Programma altijd aanpassen. Dit zal normaliter gebeuren om verbeteringen aan te brengen, doch PrivacyTeam is dit niet verplicht. Indien Klant wijzigingen in de werking wenst, dan kan Klant dit aan PrivacyTeam kenbaar maken. PrivacyTeam zal dan een en ander bekijken en bepalen of dit kosteloos gewijzigd kan worden.

2. Rechten

Klant heeft uitdrukkelijk geen rechten voor wat betreft de broncode van het Programma, noch op de inhoud van de via het Programma beschikbaar gestelde informatie, modellen en documenten. De intellectuele eigendomsrechten met betrekking tot het Programma en de informatie, modellen en documenten berusten exclusief bij PrivacyTeam. Klant mag de generieke DPIA’s gebruiken om daar een ‘eigen’ - organisatie specifieke - DPIA van te maken. Klant mag de informatie op geen enkele wijze beschikbaar stellen aan derden. Het kopiëren of verveelvoudigen van de software op een andere server of locatie (ongeacht het doel hiervan, waaronder verdere verveelvoudiging of herdistributie), dan wel het openbaar maken van beschikbaar gestelde informatie is uitdrukkelijk verboden, tenzij met schriftelijke toestemming van PrivacyTeam.

3. Database

PrivacyTeam is niet verantwoordelijk voor de database die door Klant bewerkt wordt. PrivacyTeam kan niet verantwoordelijk gesteld worden voor de inhoud, noch voor de staat waarin de database zich bevindt.

4. Schade

PrivacyTeam kan niet aansprakelijk worden gesteld en aanvaardt geen enkele aansprakelijkheid omtrent het gebruik en/of de gevolgen van het gebruik van het Programma en de beschikbaar gestelde informatie, waaronder documenten (waaronder generieke DPIA’s). Schade die is ontstaan door het gebruik van het Programma dan wel de daarmee beschikbaar gestelde informatie, van welke aard dan ook, ongeacht hoe de schade is ontstaan, alsmede gevolgschade kan nimmer op PrivacyTeam worden verhaald.

5. Problemen

Het Programma wordt gebruikt ‘zoals het is’. Als Gebruiker problemen ervaart, dan kan Gebruiker contact opnemen met Afnemer. Afnemer kan contact opnemen met PrivacyTeam. PrivacyTeam zal zich inspannen om deze problemen op te lossen.

6. Beveiliging

PrivacyTeam zorgt voor adequate technische, fysieke en organisatorische maatregelen en zal deze in stand houden om de data van Gebruiker in het Programma te beschermen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, onopzettelijk verlies, wijziging, ongeoorloofde verstrekking of toegang.

De combinatie van e-mailadres en wachtwoord is aan een natuurlijke persoon (Gebruiker) gekoppeld. Gebruiker is zelf verantwoordelijk voor het geheim houden van de inloggegevens, waaronder het wachtwoord. PrivacyTeam is nimmer verantwoordelijk voor enige geleden schade, daaronder inbegrepen gevolgschade, veroorzaakt door het gebruik van het account of het wachtwoord door onbevoegden.

7. Ter beschikkingstelling Programma

De licentie voor het gebruik van het Programma alsmede de daarmee beschikbaar gestelde informatie geldt steeds voor de periode waarvoor is betaald.

8. Bestandsgrootte en opslagruimte

Standaard wordt een ‘Fair Use Policy’ (FUP) gebruikt. Dit betekent dat Klant een hoeveelheid opslagruimte krijgt die redelijkerwijs verwacht mag worden voor de betreffende softwarelicentie.

9. Beschikbaarheid webserver

De webservers voor het Programma zijn door PrivacyTeam bij een daarvoor gespecialiseerd bedrijf in Nederland ondergebracht. Deze webservers garanderen aan PrivacyTeam een maximale beschikbaarheid. Echter: PrivacyTeam kan niet verantwoordelijk worden gesteld en aanvaardt geen enkele aansprakelijkheid indien een webserver mogelijk tijdelijk niet beschikbaar is.

10. EasyDPIA®

De door PrivacyTeam aan Klant via het Programma beschikbaar gestelde informatie, modellen en documenten (waaronder: generieke DPIA’s), zijn opgesteld naar de laatste inzichten dan wel zijn afkomstig van derde partijen (bij generieke DPIA’s). PrivacyTeam kan evenwel geen garantie geven dat door het gebruiken van de informatie volledig wordt voldaan aan alle wettelijke bepalingen en regels zoals deze van

toepassing zijn op Klant, noch kan PrivacyTeam garanderen dat een DPIA naar de toekomst toe altijd actueel zal blijven.

Klant blijft verantwoordelijk en aansprakelijk voor onder meer: het bestuur en de bedrijfsvoering van zijn bedrijf/organisatie, de adequate uitvoering van de DPIA, waarmee hij wil voldoen en aantoonbaar maken dat hij voldoet aan wet- en regelgeving, en de daarbij behorende beheersmaatregelen en acties / controles binnen de operationele- en beveiligingsprocessen van Klant en het onderhoud daarvan, de wettelijke verplichtingen en zijn eigen zakelijke aangelegenheden.

11. Bijzondere persoonsgegevens

Het Programma is niet bedoeld om bijzondere persoonsgegevens in op te slaan. In het kader van de AVG is het daarom niet toegestaan om met het Programma bijzondere persoonsgegevens te verwerken.

12. Voortzetting en opzeggen

Indien Klant de overeenkomst niet opzegt, wordt de licentie voor het Programma steeds automatisch voor eenzelfde periode verlengd. Klant kan opzeggen via de knop ‘abonnement’ in het Programma. Klant mag ook opzeggen door een bericht te sturen via de e-mail of telefonisch. De opzegging moet minimaal 1 maand vóór het aflopen van de licentieperiode door PrivacyTeam zijn ontvangen. De licentieperiode staat op de factuur vermeld.

Prijsstijgingen worden altijd tijdig aan de Klant medegedeeld, zodat Klant kan opzeggen indien deze het niet eens is met de prijswijziging.

De contactgegevens zijn:

PrivacyTeam B.V.
Amersfoortseweg 38
3951 LC Maarn Nederland
Telefoon: 033 – 200 30 83
E-mail: post@privacyteam.nl

13. Verwijderen van gegevens

Na opzegging worden de gegevens van de Klant nog gedurende 30 dagen bewaard. PrivacyTeam zal na 30 dagen alle data van de Klant van haar servers verwijderen.

14. Algemene voorwaarden

Op alle leveringen van PrivacyTeam zijn de algemene voorwaarden van toepassing. Deze zijn door de Afnemer bij het afsluiten van de licentie geaccepteerd. U kunt ze ook op de website van PrivacyTeam (www.privacyteam.nl) vinden.

15. Aanpassing Gebruiksvoorwaarden

Wij kunnen de Gebruiksvoorwaarden van tijd tot tijd bijwerken. We zullen echter nooit enige wijziging doorvoeren die een negatief effect heeft zonder voorafgaande kennisgeving aan onze klanten.

Wij zullen onze klanten op de hoogte stellen van eventuele wijzigingen door deze Gebruiksvoorwaarden bij te werken en opnieuw uit te geven via EasyDPIA®. Wij adviseren regelmatig deze gegevens te bekijken, zodat de Klant op de hoogte is van deze wijzigingen.

Data Privacy & Security Policy

1. Beleid inzake gegevensbescherming- en beveiliging

De informatie die wij verzamelen is waardevol voor onze Klant, het betreft namelijk informatie over gegevensverwerkingen en de risico's die daaraan verbonden zijn. Deze bedrijfsinformatie is vaak vertrouwelijk en moet goed beschermd worden. Tevens verwerken wij persoonsgegevens. Deze persoonsgegevens zijn 'normale' persoonsgegevens, zoals naam en e-mailadres. Er worden geen gevoelige of bijzondere persoonsgegevens verwerkt. PrivacyTeam doet er alles aan om ervoor te zorgen dat de informatie die wij verzamelen veilig wordt opgeslagen en veilig en verantwoord wordt gebruikt.

Wij verwerken persoonsgegevens enkel en alleen in opdracht van de Afnemer en/of Gebruiker. Dit beleid beschrijft de informatie die wij verzamelen, waar deze wordt opgeslagen, hoe deze wordt gebruikt en hoe deze wordt beveiligd.

Deze verklaring geldt voor EasyDPIA® en de informatie die daarin door ons wordt verwerkt.

2. Data in EasyDPIA®

EasyDPIA® is een SaaS oplossing waarmee DPIA's kunnen worden gemaakt en beheerd. Naast de gegevens van de klant worden er persoonsgegevens van de deelnemers aan een DPIA in EasyDPIA® vastgelegd. Naar keuze van de deelnemer voegt deze ook een foto van zichzelf toe. Dit is echter geheel vrijwillig. Ook worden in EasyDPIA® de gegevens m.b.t. de uitgevoerde DPIA vastgelegd, waaronder de risico's die met de verwerking samenhangen en de naar aanleiding daarvan getroffen beheersmaatregelen.

3. Welke informatie leggen we vast?

Welke informatie?	Aard van de informatie	Applicatie
Naam gebruiker	Persoonsgegeven	EasyDPIA®
E-mailadres gebruiker	Persoonsgegeven	EasyDPIA® Postmark
IP-adres	Persoonsgegeven	EasyDPIA®
Foto gebruiker	Persoonsgegeven	EasyDPIA®

Bedrijfsnaam	Zakelijke informatie	EasyDPIA®
Bedrijfsgegevens	Zakelijke informatie (gegevens m.b.t. de bedrijfsvoering behorend bij de) verwerking van persoonsgegevens).	EasyDPIA®
Betaalgegevens	Zakelijke(financiële) informatie	Stripe

4. Waar wordt de informatie opgeslagen en wie heeft toegang tot de informatie?

De informatie die we ontvangen leggen we vast in een aantal applicaties:

Applicatie	Omschrijving	Hosting	Toegankelijk voor
EasyDPIA®	SaaS applicatie	LinQhost (NL)	-medewerkers MaxiCMS -medewerkers LinQhost -medewerkers PrivacyTeam
Stripe	SaaS applicatie voor betaaldiensten	AWS (US)	-medewerkers MaxiCMS -medewerkers PrivacyTeam
Postmark	Mail service	AWS (US)	-medewerkers MaxiCMS -medewerkers PrivacyTeam

PrivacyTeam heeft met de leveranciers van de applicaties afspraken gemaakt om de informatie (waaronder persoonsgegevens) op een adequate manier te beveiligen. Indien er gegevens worden opgeslagen buiten Europa zijn met de leveranciers afspraken gemaakt via Standard Contractual Clauses (SCC).

Via Postmark en Stripe worden persoonsgegevens verwerkt in de Verenigde Staten. Sinds de Schrems II uitspraak van juli 2020 van het Europese Hof van Justitie, wordt de VS als ‘niet adequaat’ aangemerkt en is het zonder een aanvullend risicoassessment niet toegestaan persoonsgegevens te laten verwerken in de Verenigde Staten.

Door PrivacyTeam is in aanvulling op de SCC een Data Transfer Impact Assessment (DTIA) uitgevoerd. Omdat er alleen sprake is van gegevensverwerking van een zakelijk e-mailadres en namen, en er derhalve geen gevoelige en/of bijzondere persoonsgegevens worden verwerkt, is er geen sprake van een hoog privacy risico. Hierdoor is de gegevensverwerking zoals hierboven vermeld toegestaan. De uitkomsten van de DTIA kunnen wij op verzoek beschikbaar stellen.

Beschrijving van de maatregelen om te waarborgen dat enkel bevoegd personeel van PrivacyTeam toegang heeft tot de verwerking van Persoonsgegevens.	
Medewerkers en gegevens:	**Handelingen:**
Medewerkers hebben toegang tot de licentie-informatie. Zij kunnen onder meer zien welke licentie is afgenomen en de bijbehorende contractduur.	Administratieve handelingen in het kader van licenties. Ondersteuning van de eindgebruiker.
Medewerkers hebben toegang tot de klant informatie.	Ondersteuning van de eindgebruiker.
Medewerkers hebben toegang tot de betalings-informatie. Zijn kunnen onder meer contactgegevens en betalingsgegevens inzien.	Administratieve handelingen in het kader van de licenties. Ondersteuning van de eindgebruiker.
IT-databeheerders hebben toegang tot de databases.	De handelingen van IT-databasebeheerders zijn gericht op continuïteit en optimalisatie van ICT-systemen.

Dit betreft telkens een beperkt aantal medewerkers dat toegang heeft tot de informatie (‘need to know’ basis). De medewerkers die toegang hebben tot de informatie hebben allen een geheimhoudingsovereenkomst getekend.

5. Hoe lang wordt de informatie bewaard?

Type	Informatie	Acties	Bewaartermijn
EasyDPIA®	Gegevens Gebruiker	Account verwijderen	Direct verwijderd
	Gegevens klant (w.o. DPIA’s)	Beëindigen licentie	30 dagen
Stripe	Betaalgegevens	Beëindigen licentie	7 jaar
Postmark	E-mails	-	30 dagen

6. Met wie delen we de informatie?

De informatie wordt niet met andere derden gedeeld anders dan op grond van hetgeen in deze voorwaarden is genoemd, dan op grond van een wettelijke bepaling of een rechterlijke uitspraak, dan wel wanneer PrivacyTeam gehouden is vertrouwelijke informatie aan door de wet of de bevoegde rechter aangewezen derde(n) te verstrekken, en PrivacyTeam zich ter zake niet kan beroepen op een wettelijk dan wel door de bevoegde rechter erkend of toegestaan recht van verschoning.

7. Hoe wordt de informatie beveiligd?

PrivacyTeam zal zich steeds en doorlopend inspannen voldoende technische en organisatorische maatregelen te nemen om de informatie tegen verlies of tegen onbevoegde kennisname, aantasting of wijziging te beschermen.

Versleuteling	Alle netwerkverbindingen met de webserver zijn beveiligd met TLS-encryptie. De certificaten worden extern beheerd door LinQhost. Zij kopen ons certificaat in bij Sectigo. Zelf hebben we geen beschikking tot de certificaatfile.
	De data op de server zijn versleuteld met AES-256-CBC.
	De sleutel wordt encrypted opgeslagen buiten de software (double key encryption).
	Wachtwoorden worden versleuteld opgeslagen met Argon2id.
Identiteits- en toegangsbeheer	De gebruiker wordt verplicht om tweefactor-authenticatie in te stellen.
	Een account wordt na vijf pogingen om in te loggen met een onjuist wachtwoord bij iedere volgende poging vergrendeld voor een steeds langere periode.
	Accounts zijn gekoppeld aan individuen, er zijn geen gedeelde systeemaccounts.
Serverbeveiliging en- hardening	De webserver wordt middels firewalls beschermd tegen netwerk gebaseerde aanvallen vanaf het internet.
	Het gehele online platform is voorzien van actuele security-updates.
	Voor het maken van Back-ups is een SLA afgesloten en back-ups worden zeer regelmatig gemaakt.
Beveiliging webapplicatie	De webapplicatie wordt beschermd tegen verschillende soorten aanvallen, zoals XSS, SQLi, RFI, LFI, User Agent etc.

	De firewall blokkeert ook herhaalde aanvallen en stuurt meldingen wanneer een aanval wordt gedetecteerd. Bovendien zal het mislukte aanmeldingen loggen en het IP-adres blokkeren na een aantal pogingen.
Hosting	Onze services (database, API, etc.) zijn gehost in een ISO 27001-gecertificeerd datacenter.
Logging en monitoring	Het detailniveau van logging is voldoende groot om bij aanvallen ingezet te worden teneinde de handelswijze en netwerkidentiteit van de aanvaller te achterhalen.
	Kritieke systeemfuncties worden gemonitord en verstoringen worden gemeld aan systeembeheerders en opgevolgd middels een “lerend” monitoring- en alertingsysteem.
Veilig beheer	Toegang op afstand tot servers is meervoudig beveiligd.
	Er is een adequaat back-up plan en restoreplan uitgewerkt.
Testen	PrivacyTeam test regelmatig de beveiliging van Het Programma.
Patches	PrivacyTeam zorgt ervoor dat security patches zodra deze beschikbaar komen worden geïnstalleerd.
Beleid	PrivacyTeam heeft een Informatiebeveiligingsbeleid.
Medewerkers	Met medewerkers worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt.
	PrivacyTeam stimuleert bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
	Medewerkers hebben op grond van een autorisatiesystematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.

8. Hoe gaan wij om met de rechten van betrokkenen?

In de situatie dat PrivacyTeam verwerker is van persoonsgegevens geldt het volgende: indien een betrokkene een verzoek tot uitoefening van zijn/haar wettelijke rechten richt aan PrivacyTeam, is PrivacyTeam niet bevoegd tot het direct afhandelen van een verzoek van de betrokkene. PrivacyTeam zal enkel bijdragen tot het inwilligen van de verzoeken welke afkomstig zijn van de Klant.

In de situatie dat PrivacyTeam verwerkingsverantwoordelijke is van persoonsgegevens geldt het volgende: de privacywetgeving geeft iedereen wiens persoonsgegevens worden verwerkt een aantal rechten om

ervoor te zorgen dat de verwerking van persoonsgegevens op een eerlijke en transparante manier geschiedt.

U heeft de volgende rechten:

- uitleg krijgen over welke persoonsgegevens we verwerken;
- inzage in de precieze persoonsgegevens die we verwerken;
- het laten corrigeren van fouten;
- het laten verwijderen van verouderde persoonsgegevens;
- intrekken van uw toestemming;
- bezwaar maken tegen een bepaald gebruik.

U kunt uw recht gebruiken door een schriftelijk verzoek bij ons in te dienen. Het is hierbij belangrijk dat u zich kunt legitimeren en kunt aantonen dat het verzoek daadwerkelijk betrekking heeft op uw eigen persoonsgegevens. Het is niet toegestaan om de persoonsgegevens van anderen op te vragen. Wij beslissen binnen één maand op uw verzoek. Bij veel of ingewikkelde verzoeken mogen wij deze termijn gemotiveerd met maximaal twee maanden verlengen. Bij uitgebreide verzoeken kunnen wij u kosten in rekening brengen.

9. Wat doen we bij een incident?

PrivacyTeam zal de klant zonder onredelijke vertraging informeren over inbreuken op de beveiliging volgens artikel 33 van de AVG.

PrivacyTeam deelt ten minste de volgende informatie wanneer zich een incident of een datalek voordoet:

- de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;
- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die zijn genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Voor een uitgebreide beschrijving van hoe PrivacyTeam als Verwerker persoonsgegevens verwerkt, verwijzen wij u naar de Verwerkersovereenkomst, welke is opgenomen in de Algemene Voorwaarden.

Cookieverklaring

EasyDPIA® is een webapplicatie en geen website. Alleen de inlog en registreer pagina maken gebruik van een internetadres om de toegang tot de applicatie mogelijk te maken.

Om gebruik te maken van EasyDPIA® worden door PrivacyTeam B.V. alleen noodzakelijke cookies gebruikt. Hiervoor is geen voorafgaande toestemming van de Gebruiker vereist.
De volgende Cookies worden gebruikt:
Een sessie cookie en een XSRF-Token.

- Een sessie cookie wordt geplaats om EasyDPIA® goed te laten functioneren (functionele cookie). Deze slaat tijdelijk (tijdens de sessie) gegevens op.

- Een XSRF-Token is een beveiligingsmaatregel en dient ervoor om zogenaamde ‘cross-injecties’ tegen te gaan. Ook dit is een noodzakelijke cookie om een veilig gebruik van EasyDPIA® te bewerkstelligen.

EasyDPIA® gebruikt geen analytische- of trackingcookies.