Versie: 1.3/ 2024-07-17

Verwerkers-overeenkomst MindYourPass B.V.

Bestaande uit:

Deel 1. Data Pro Statement

Deel 2. Standaardclausules voor verwerkingen

Deel 1: Data Pro Statement

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst voor het product of de dienst van het bedrijf dat dit Data Pro Statement heeft opgesteld.

Algemene informatie

1. **Dit Data Pro Statement is opgesteld door de volgende data processor (verwerker):**
   MindYourPass B.V.
   High Tech Campus 27
   5656 AE Eindhoven

   Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met:

   Fabian Doodkorte
   fabian.doodkorte@mindyourpass.com
   06-10983764

2. **Dit Data Pro Statement geldt vanaf** 2024-07-17
   Dit Data Pro Statement en de daarin omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van data protectie steeds voorbereid en actueel te blijven. Wij houden u op de hoogte van eventuele nieuwe versies via onze website. Tevens sturen wij deze nieuwe versies naar onze opdrachtgever(s) op.

3. **Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor**

   MindYourPass Password Firewall
   MindYourPass Cyber Dashboard
   MindYourPass Password Generator B2B

4. **Omschrijving product/dienst**
   Deze verwerkersovereenkomst betreft de volgende drie producten van MindYourPass. Gezamenlijk worden deze hierna ook aangeduid als **'onze/deze producten'**. Wanneer bepaalde specificaties in deze verwerkersovereenkomst slechts van toepassing zijn op één van de producten van MindYourPass zal dit worden aangegeven.

   MindYourPass Password Firewall. Deze applicatie, bedoeld voor B2B-relaties, monitort waar ingelogd wordt en wat de kwaliteit van de gebruikte wachtwoorden is. Afhankelijk van het door de opdrachtgever gekozen abonnement, kan het de toegang tot accounts met zwakke wachtwoorden blokkeren.
   MindYourPass Cyber Dashboard. Deze applicatie, bedoeld voor B2B-relaties, geeft inzicht in de accounts die door de medewerkers van een organisatie gebruikt worden en de kwaliteit van de gebruikte wachtwoorden. Tevens geeft deze applicatie inzicht in de ontwikkeling na verloop van tijd van de cyberveiligheid op het gebied van onlineaccounts.
   MindYourPass Password Generator B2B. Deze applicatie, bedoeld voor B2B-relaties, genereert unieke en zeer sterke wachtwoorden uit o.a. een voor de gebruiker eenvoudig te onthouden wachtwoord.

Wachtwoorden worden steeds opnieuw gegenereerd op het moment dat de gebruiker wil inloggen. Hierdoor hoeven de gegenereerde wachtwoorden niet opgeslagen te worden.

5. **Beoogd gebruik**

Onze producten zijn ontworpen vanuit de concepten “Privacy by design” en “Security by design”. Om die reden worden gebruikers geanonimiseerd en worden e-mailadressen slechts tijdelijk opgeslagen en daarna verwijderd, en worden er geen andere persoonsgegevens opgeslagen. Deze overige gegevens die worden opgeslagen zijn license keys (in de vorm van global unique identifiers), URLs, kwaliteitsscores van wachtwoorden, client ID’s (in de vorm van global unique identifiers) en time stamps. Wij zien dit niet als persoonsgegevens. Indien en voor zover dit toch gezien wordt als het verwerken van persoonsgegevens is deze verwerkersovereenkomst van toepassing.

Mocht MindYourPass op enig moment het e-mailadres tijdens registratie en inloggen nodig hebben, dan zal het op dat moment de gebruiker vragen deze gegevens te verstrekken. MindYourPass gebruikt deze gegevens dan alleen voor het uitvoeren van de aangegeven handeling (zoals een inlog-procedure) en verwijdert deze gegevens daarna direct.

MindYourPass houdt bij deze producten geen rekening met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of door de overheid uitgegeven persoonsnummers.

6. **Data processor heeft bij het ontwerpen van deze producten privacy by design/privacy by default op de volgende wijze toegepast:**

Onze producten zijn van de grond af aan zo ontworpen dat er geen persoonsgegevens opgeslagen hoeven te worden. Als persoonsgegevens nodig zijn worden deze op dat moment aan de gebruiker gevraagd, en nadat deze niet meer nodig zijn worden deze gegevens direct verwijderd. Zo wordt bijvoorbeeld tijdens registratie en inloggen om een e-mailadres gevraagd, maar wordt deze slechts tijdelijk opgeslagen en verwijderd zodra het account is aangemaakt of er is ingelogd.
Anders dan een traditionele wachtwoordmanager, slaat MindYourPass via het product Password Generator B2B geen wachtwoorden op maar genereert het deze opnieuw op het moment dat ze nodig zijn. Er is dus geen sprake van een (digitale) kluis met bijbehorende risico’s.
Omdat MindYourPass geen persoonsgegevens opslaat, kan in de producten gebruik worden gemaakt van one-way versleuteling (hashing). Dit is significant veiliger omdat er (per definitie) geen sleutel bestaat om de versleutelde informatie te ontsleutelen. Bij onze producten worden gebruikersnamen gepseudonimiseerd door daar license keys voor te genereren. De opdrachtgever bewaart de koppelingen tussen de license keys en de gebruikersnamen. MindYourPass heeft alleen toegang tot de license keys, niet tot deze koppelingen. De opdrachtgever is zelf verantwoordelijk voor een veilige en adequate beveiliging van de koppelingen.

7. **Data processor gebruikt de Standaardclausules voor verwerkingen, welke als bijlage bij de Overeenkomst te vinden zijn.**

8. **MindYourPass verwerkt de persoonsgegevens van zijn opdrachtgevers binnen de EU/EER.**

9. **Data processor maakt gebruik van de volgende sub-processors:**

Sub-processor	**Doelbinding**	**Data binnen EU/EER**	**Maatregelen gegevensbescherming**
MailJet (https://mailjet.com/).	Verwerking van e-mailadressen via MindYourPass Password Generator B2B	Ja	https://www.mailjet.com/security-privacy/
Google Cloud (https://cloud.google.com/)	Hosting MindYourPass producten en data-opslag	Ja	https://privacy.google.com/intl/nl/businesses/

10. **MindYourPass ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen:**
Opdrachtgever kan door middel van het sturen van een e-mail naar info@mindyourpass.com een verzoek tot inzage, correctie, verwijdering of dataportabiliteit indienen bij MindYourPass. Bij een dergelijke verzoek neemt MindYourPass binnen 3 werkdagen contact op met opdrachtgever ter afstemming van het verzoek.

11. **MindYourPass zal op de volgende wijze medewerking verlenen aan Data Privacy Impact Assessments:**
MindYourPass verleent, zo volledig mogelijk en voor zover redelijkerwijs van data processor verwacht kan worden, medewerking aan het uitvoeren van een Data Privacy Impact Assessment (DPIA). Hierin ondersteunt MindYourPass de uitvoer van het DPIA door het verstrekken van alle benodigde informatie over door data processor genomen beveiligingsmaatregelen ter waarborging van de privacy bij gegevensverwerking.

12. **Na beëindiging van de Overeenkomst met een opdrachtgever verwijdert data processor de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen 3 maanden op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible), of zullen deze persoonsgegevens op verzoek binnen 3 maanden worden geretourneerd.**
Behalve bij het registreren en het inloggen verwerkt MindYourPass geen persoonsgegevens. Het e-mailadres dat tijdens registratie en inloggen gebruikt wordt, wordt tijdelijk opgeslagen en daarna verwijderd. Indien en voor zover opdrachtgever van mening is dat MindYourPass overige persoonsgegevens verwerkt, worden deze na beëindiging van de Overeenkomst met een opdrachtgever in principe binnen 3 maanden op zodanige wijze verwijderd dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (render inaccessible). Tevens kunnen op verzoek de gegevens na beëindiging van de Overeenkomst met opdrachtgever geretourneerd worden. Data processor zal dan per e-mail een zipfile sturen met de betreffende gegevens.

13. **Met de opdrachtgever zijn geen specifieke afspraken gemaakt omtrent het retourneren van door data processor verwerkte persoonsgegevens.**

Beveiligingsbeleid

14. **Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn product of dienst:**

- *Hoe wordt vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van het product of de dienst geborgd;*
  Vertrouwelijkheid en integriteit worden geborgd doordat MindYourPass niet over persoonsgegevens beschikt. Vertrouwelijkheid en integriteit komen hiermee nimmer in het geding. Beschikbaarheid en veerkracht worden geborgd doordat MindYourPass een volledig schaalbare oplossing is die op basis van state-of-the-art technologieën in de Cloud draait. Hierbij vormt MindYourPass zelf een SaaS-oplossing, maar maakt deze intern gebruik van PaaS oplossingen (Kubernetes). Hierdoor kan MindYourPass beschikken over alle in gebruik zijnde mechanismen om de beschikbaarheid en de veerkracht van MindYourPass te kunnen waarborgen. Zie ook onder punt 6 hoe MindYourPass privacy by design/privacy by default waarborgt.

- *Hoe wordt geborgd dat bij een incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig hersteld wordt.*
  MindYourPass draait als een verzameling microservices in een Kubernetes cluster. Het Kubernetes cluster wordt gehost bij Google in een Nederlands datacentrum. Deze opzet zorgt ervoor dat de beschikbaarheid van MindYourPass op alle mogelijke fronten gewaarborgd wordt. Mocht er toch een incident plaatsvinden dan biedt deze opzet tevens uitgebreide mogelijkheden om een incident te identificeren en om alle services operationeel te houden en/of weer in de lucht te brengen. MindYourPass is ontworpen om zoveel mogelijk gebruik te maken van standaard oplossingen die zich in de praktijk bewezen hebben. MindYourPass heeft hiervoor ook externe deskundigheid ingeschakeld om ontwerpen te maken en/of de bestaande ontwerpen en implementaties te valideren.

15. **Data processor heeft zich geconformeerd aan het volgende Information Security Management System (ISMS):**
MindYourPass is sinds 18 december 2023 ISO27001:2022 gecertificeerd welke dienst doet als ISMS. Daarnaast heeft MindYourPass de ambitie om in de toekomst aan meerdere normeringen te voldoen. Momenteel volgt MindYourPass de volgende normeringen:
    - ISO27001:2022;
    - OWASP;
    - NCSC Webrichtlijnen.

16. **Data processor heeft de volgende certificeringen:**
MindYourPass heeft de ambitie om aan meerdere certificeringen te voldoen. Momenteel beschikt MindYourPass reeds over de volgende certificering(en):
    - Data Pro Certificaat
    - ISO27001:2022
    - ISAE 3000

Datalekprotocol

17. **In geval er toch iets misgaat, hanteert data processor een datalekprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten.**
MindYourPass heeft een intern datalekkenprotocol vastgesteld om datalekken te ontdekken, te voorkomen en te dichten. In het geval van een datalek zal MindYourPass haar opdrachtgevers per e-mail en/of telefoon op de hoogte stellen van het incident. MindYourPass zal zelf geen meldingen doen van een datalek aan de AP of aan betrokkenen. Het wel of niet melden aan hen blijft de verantwoordelijkheid van de opdrachtgever.

MindYourPass zal de opdrachtgever desgewenst en voor zover mogelijk ondersteunen bij het meldproces, door de volgende informatie (wanneer van toepassing) te delen met opdrachtgevers:
- specificatie van het incident
- samenvatting van het incident
- eventueel betrokken sub-processors
- hoeveel personen er zijn betrokken bij het datalek
- omschrijving van de groep betrokkenen bij het datalek
- tijdstip van het datalek
- aard van het datalek
- om welke type persoonsgegevens het gaat
- welke gevolgen de inbreuk kan hebben voor de persoonlijke levenssfeer van betrokkenen
- de vervolgacties naar aanleiding van het datalek
- de gehanteerde technische beschermingsmaatregelen ten tijde van het ontdekken van het datalek
- eventuele internationale aspecten