Gegevensbescherming

Gegevensbescherming

iASSET Heeft een uitvoerig gegevensbeschermingsbeleid. Dit heeft als doel:

- Als handleiding voor onze functionarissen voor gegevensbescherming,
- Als achtergronddocument voor de gegevensverwerkingsovereenkomst met de gegevensbeschermingsfunctionarissen van onze klanten,
- Als handleiding voor onze medewerkers.
- Om te voldoen aan de privacy gerelateerde wetgeving

Hier staat de volledige (engelstalige) Data Protection Policy. Hieronder staan de belangrijkste punten uit dat document.

Wie is de gegevensbeschermingverantwoordelijke

Verantwoordelijk voor het opstellen en naleven van het gegevensbeschermingsbeleid is de gegevensbeschermingverantwoordelijke (data protection Officer, afgekort: DPO): Robbert Bloksma

Welke gegevens betreft het

iASSET slaat voornamelijk gegevens op over de door opdrachtgever beheerde objecten. In het geval van meldingen met juridische opvolging kunnen daar persoonsgegevens bij betrokken zijn. Om authorisatie, workflow processen en communicatie mogelijk te maken slaan we enkele persoonsgegevens op. Een inventarisatie is te vinden in onze privacyvoorwaarden.

Het is iASSET toegestaan om de gegevens in de databases van iASSET te gebruiken ter verdere verbetering van het product. Bijvoorbeeld in de vorm van algoritmen ten behoeve van predictive maintenance. Opdrachtgever geeft iASSET toestemming voor dit gebruik. iASSET dient er daarbij voor zorg te dragen dat de resultaten op geen enkele wijze te herleiden zijn naar de opdrachtgever.

Waar zijn de gegevens

De gegevens worden bewerkt en bewaard op de servers van TransIP B.V. in Nederland. Alle apparatuur waar persoonsgegevens op kunnen staan is geregistreerd. Diverse Cloudproducten worden gebruikt bij onze interne en communicatieprocessen. We houden bij met wie van deze externe verwerkers we een GDPR waardige verwerkersovereenkomst hebben en zijn actief aan het opvolgen om van de rest deze ook te krijgen.

De medewerkers zijn bekend met de restrictie dat alleen geregistreerde producten en apparaten mogen worden gebruikt.

Wie heeft toegang tot de gegevens

Persoonsgegevens zijn alleen toegankelijk voor werknemers die hiertoe bevoegd zijn. In hun contracten staat een geheimhoudingsclausule.

Niet-persoonsgegevens worden gedeeld met partners en intern gebruikt voor analyse om onze producten nog beter te maken

Welke risico’s zijn verbonden aan de gegevens

Over het algemeen zijn de gegevens in iASSET laag privacy gevoelig. Het betreft immers vooral gegevens over objecten in de openbare ruimte, gegevens die in principe openbaar zijn.

Qua persoonsgegevens hebben we naast naam en login een categorie die gevoeliger ligt: bij meldingen kunnen gegevens of foto’s van verkeersverdachten of -slachtoffers zijn opgeslagen.

Wat doen we om corruptie, onrechtmatige toegang of verlies te voorkomen

In het originele document worden meer dan een dozijn maatregelen genoemd om corruptie, onrechtmatige toegang of verlies te voorkomen. De belangrijkste hiervan zijn hieronder opgenoemd.

- We gebruiken anti-virussoftware, DDoS bescherming en firewalls. Alle software wordt maandelijks bijgewerkt naar de nieuwste versies.
- Er wordt dagelijks gebackupped en de backups worden offsite bewaard.
- We beheren en delen onze wachtwoorden veilig met een specifiek wachtwoordbeheersysteem. Bij beëindiging van het dienstverband van een medewerker worden zijn/ haar accounts geblokkeerd of verwijderd. Gedeelde sleutels (ook bijvoorbeeld alarmsysteem kantoor) worden veranderd en alleen gedeeld met de blijvende werknemers.
- Alle verbindingen van en naar buiten zijn versleuteld. Gegevensdragers in gegevensverwerkende hardware moeten zijn versleuteld zodat zij zonder sleutel onbruikbaar zijn zowel in als buiten de gegevensverwerkende hardware .
- Bij tijdelijk verlaten van een werkplek zijn alle papieren gegevensdragers welke persoonsgegevens bevatten uit zicht opgeborgen. Bij verlaten van een werkplek aan het einde van de dag zijn alle papieren gegevensdragers welke persoonsgegevens bevatten opgeborgen achter een slot.
- Vóór verkoop of weggooien van gegevensverwerkende hardware moeten gegevensdragers daarin veilig zijn gewist. Dat houd in tenminste geheel overschreven met 0 waarden.

Wat doen we om de gevolgen van een onverhoopt gegevenslek te beperken

Er is een datalek meldprocedure. In grote lijnen is dit:

1. Onderzoek de aard van de mogelijk gelekte gegevens
2. Indien persoonlijke gegevens zijn betrokken, informeer de personen wie het betreft en hun werkgever en registreer het incident in het datalek register.
3. informeer maximaal 72 later de Autoriteit Persoonsgegevens.

Wat doen we om dit beleid levend te houden

Elke 6 maanden verzoekt de DPO alle gebruikers om te controleren of de technische beveiligingen nog steeds zijn ingeschakeld, up-to-date zijn en geen fouten in hun logbestanden bevatten.

Om ervoor te zorgen dat dit beleid bekend is bij en wordt toegepast door alle werknemers en om ervoor te zorgen dat het up-to-date is, voert de DPO jaarlijks een controle uit. Dit bestaat minimaal uit het volgende.

- Een audit op de toepassing van het beleid door alle werknemers inclusief het management.
- Een audit van de geautomatiseerde preventieprocedures.
- Een recensie en update van dit document en de Wiki-pagina’s over het onderwerp.
- Een jaarlijkse informatiebijeenkomst waarin veranderingen worden uitgelegd en iedereen op de hoogte blijft van het beleid.