MAART 2018

Uw organisatie & AVG

Beste klant,

Als gebruiker van PE-online is het zeer waarschijnlijk dat u persoonsgegevens verwerkt. Vanaf 25 mei 2018 treedt de nieuwe Europese wet op dit gebied in werking. Deze wet wordt in Nederland de AVG (Algemene verordening gegevensbescherming) of in Europa de GDPR (General Data Protection Regulation) genoemd en heeft betrekking op iedere organisatie die persoonsgegevens verwerkt.

Omdat wij als leverancier van PE-online betrokken zijn bij de verwerking van uw gegevens willen wij u een aantal handvaten en aandachtspunten geven welke u kunt gebruiken als u hiermee aan de slag gaat. Bij twijfel is het altijd slim om een expert te raadplegen.

Relatie

De relatie tussen uw organisatie en Xaurum is voor wat betreft de AVG respectievelijk een datacontroller (databeheerder) en dataprocessor (dataverwerker) relatie met als applicatie PE-online. U bent eigenaar van de data welke u verwerkt en Xaurum zal deze opslaan en verwerken volgens de gemaakte afspraken.

Scope

De wet AVG gaat niet alleen over het verwerken van klantgegevens, maar omvat alle verwerking van persoonsgegevens binnen uw organisatie. Denk hierbij dus ook aan personeel in de vorm van bijvoorbeeld salarisverwerking en verzekeringen maar ook aan externen die toegang hebben tot uw data of waaraan u data versterkt.

Doel

Overal waar u persoonsgegevens opslaat dwingt de AVG u om dit te beperken. Waar vroeger vaak extra informatie over personen werd gevraagd omdat dit in de toekomst wel eens handig kon zijn wordt dit onder de nieuwe AVG wet een stuk lastiger. U dient namelijk te beschrijven welk doel het vragen van dit gegeven heeft. U heeft een verantwoordingsplicht. Dit brengt ons bij het verwerkingsregister.

Verwerkingsregister

In een verwerkingsregister beschrijft u onder andere wie er bij u welke verwerkingen doet en waarom. Het doel van de verwerking kan bijvoorbeeld een openbaar register zijn, marketing of dataverzameling voor een instantie. Ook legt u vast met wie u data deelt. Daarnaast staat hierin welke gegevens er per verwerking worden opgeslagen of gedeeld. Tenslotte dient in het verwerkingsregister te staan welke technische en organisatorische maatregelen u heeft genomen om deze persoonsgegevens te beveiligen.

Privacy statement

Wanneer u persoonsgegevens verzamelt conform het verwerkingsregister dan dient u de persoon in kwestie hiervan op de hoogte te stellen. Hiervoor kunt u een privacy statement ofwel verklaring opstellen. Deze verklaring geeft aan wat u met welke persoonsgegevens zal gaan doen.

Een akkoord op dit statement dient u te verkrijgen via het opt-in principe. Dit houdt in dat men onder de nieuwe AVG wet dient te werken met een actieve akkoordverklaring.

Overeenkomsten

Omdat u als gebruiker van PE-online de data laat beheren door Xaurum en wellicht nog te maken heeft met andere partijen (CRM leverancier, salarisverwerker) waar u persoonsgegevens mee uitwisselt is het verstandig hier afspraken over vast te leggen. Een gebruikelijke manier hiervoor is de dataverwerkers overeenkomst. Hierin staan duidelijk de afspraken tussen de eigenaar van de data (uw organisatie) en de instantie wie u de verwerking en opslag toevertrouwt (Xaurum). Xaurum kan u van voorbeelden voorzien.

Omgang met data

Wettelijk gezien moet u veilig met uw data omgaan. Het is verstandig een duidelijk beeld te hebben van de beveiligingsmaatregelen die u en uw leveranciers hebben voor het beheer van uw data. Denk hierbij aan het versleuteld opslaan van gegevens, geheimhoudingsplicht, veilige hardware & datacentra, continuïteitsregeling en interne procedures.

Daarnaast is het van belang dat u beleid ontwikkelt op het gebied van procedures. Welke data verspreid u handmatig (bijvoorbeeld rapporten), bevatten deze persoonsgegevens en hoe zorgt u dat deze veilig bij de ontvanger aankomen?

Ook wordt u geacht na te denken over de toegang die diverse personen binnen uw organisatie hebben. Kan iedereen zien wat nodig is of zijn er mensen die teveel gegevens kunnen inzien (voorbeeld: een directeur hoeft niet alle data in te zien wanneer hij hier in de regel niets mee doet).

Anonimisering en verwijdering

Een persoon kan u vragen om de persoonsgegevens te verwijderen. U dient duidelijk in kaart te brengen welke gegevens u op dat moment dient te anonimiseren en / of verwijderen. Als dit een veel voorkomende vraag is kunt u dit laten automatiseren door uw leverancier. Let hierbij ook op bijlagen en inhoud hiervan.

Anonimiseren houdt in dat u alle persoonsgegevens wijzigt zodat deze nooit meer te herleiden zijn naar deze persoon. Het verwijderen van gegevens houdt in dat u deze niet meer zichtbaar in de administratie heeft. Het vernietigen van persoonsgegevens houdt in dat deze ook niet meer voor archiefdoeleinden beschikbaar zijn.

Meldplicht

Mochten er persoonsgegevens lekken dan heeft u onder de AVG (en ook de huidige) wet een meldplicht. Daarnaast dient u dit vanaf 25 mei ook te documenteren. De meldplicht omvat een tijdspanne van 72 uur (Let hier op in uw verwerkingsovereenkomst. Als uw leverancier hier lang over doet dan resteert u minder tijd).

Xaurum en PE-online

Om uw data veilig te stellen heeft Xaurum diverse maatregelen getroffen, welke hieronder kort worden toegelicht. Vraag uw projectmanager om het totaaloverzicht.

- Verwerkersovereenkomst
- OWASP
  De applicatie PE-online wordt regelmatig (minstens 4x per jaar) blootgesteld aan een OWASP-scan (Open Web Application Security Project). OWASP scant de applicatie op mogelijke veiligheidslekken.
- Applicatiebeheer
- PE-online wordt ontwikkeld volgens meerdere stadia. Er wordt gewerkt met een ontwikkel, test en productieomgeving. Iedere nieuwe ontwikkeling aan de applicatie doorloopt deze stadia waar uiteraard getest wordt op functioneel en data niveau.
  De ontwikkeling gebeurt in een Microsoftomgeving (.NET & SQLserver).
- Escrow
  Xaurum heeft een Escrow regeling met Escrow4All. Iedere klant neemt hier automatisch (en kostenloos) aan deel. De Escrow regeling biedt onze klanten zekerheid van continuïteit op het moment dat Xaurum dit zelf niet meer zou kunnen garanderen.
- ISO27001
  In 2018 wil Xaurum een ISO27001 certificering behalen. Hiervoor zijn alle werkzaamheden reeds in de afrondende fase en heeft er al een proefaudit plaatsgevonden. De definitieve audit start juni 2018.
- Toegangsbeleid
  Toegang tot data, updatebeleid van laptops, gebruik van (legitieme) software is allemaal beschreven in de ISO27001 documentatie en wordt centraal beheerd.
- Medewerkers
  Alle medewerkers van Xaurum zijn bekend met het voor hun van toepassing zijnde beleid uit de ISO27001. Ook heeft iedereen een geheimhoudingsverklaring getekend.
- Hardware
  PE-online en uw data is opgeslagen in 2 datacentra op verschillende locaties. Alle hardware is dubbel uitgevoerd en eigendom van Xaurum. Systemen zijn van erkende leveranciers (Dell, Juniper). Backups worden regelmatig gemaakt.

- Beveiligde bestandsuitwisseling
  Xaurum en PE-online ondersteunen diverse beveiligde verbindingen zoals webservices maar ook bestandsoverdrachten via een beveiligde FTP verbinding. Wanneer u niet weet of u gebruik maakt van een beveiligde FTP verbinding neem dan contact op met uw projectmanager.

Handige links

- https://privacycompass.nl/
  Wanneer u geïnteresseerd bent in een snelle scan van uw organisatie, een workshop of een uitgebreide doorlichting op het gebied van AVG / GDPR.
- FGDichtbij
  Een doe-het-zelf gereedschap waarmee jij je organisatie met een duidelijk stappenplan gereed maakt voor de nieuwe privacywet.
- https://autoriteitpersoonsgegevens.nl/
  De website met een bron van informatie over de nieuwe AVG / GDPR wet.
- https://rvo.regelhulpenvoorbedrijven.nl/avg/welkom
  Een online checklist waarmee u een zelfscan kunt doen.
- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleidingalgemeneverordeninggegevensbescherming.pdf
- https://whitewire.be/templates/
  Gratis templates gerelateerd aan AVG / GDPR.

Met vriendelijke groet,
Xaurum