AVG checklist

Samenvatting van de belangrijkste aspecten van de AVG.
U kunt deze gebruiken als checklist voor de implementatie van de juiste maatregelen om AVG compliant te worden.

Op 25 mei 2018 is de nieuwe privacywetgeving AVG (GDPR) van kracht. Dit betekent dat organisaties meer verantwoordelijkheid hebben bij het vastleggen en gebruiken van privacygevoelige gegevens.
Om te voldoen aan de AVG moet u als organisatie een aantal maatregelen treffen. Hieronder hebben wij de maatregelen die nodig zijn om aan de AVG te voldoen beknopt toegelicht.

Privacybeleid

Stel een privacybeleid op dat de richting, principes en de basisregels omschrijft voor de persoonsgegevensverwerking die uw organisatie voor haar activiteiten doet.

Rechten van betrokkenen

De personen of organisaties waarvan u persoonsgegevens verwerkt worden in de context van de AVG ‘betrokkene’ genoemd. Betrokkenen hebben een aantal rechten waar ze beroep op kunnen doen. De rechten zijn de volgende:

- Het recht op dataportabiliteit. Het recht om persoonsgegevens over te dragen;
- Het recht op vergetelheid. Het recht om ‘vergeten’ te worden;
- Recht op inzage. Dat is het recht van mensen om de persoonsgegevens die u van hen verwerkt in te zien;
- Recht op rectificatie en aanvulling. Het recht om de persoonsgegevens die u verwerkt te wijzigen;
- Het recht op beperking van de verwerking: Het recht om minder gegevens te laten verwerken;
- Het recht met betrekking tot geautomatiseerde besluitvorming en profilering. Oftewel: het recht op een menselijke blik bij besluiten;
- Het recht om bezwaar te maken tegen de gegevensverwerking;

U bent verplicht een procedure op te stellen die ervoor zorgt dat als een betrokkene zich beroept op één of meerdere rechten, de uitvoering van deze rechten effectief tot uiting komen.

Register van verwerkingen

Onder de AVG heeft uw organisatie een verantwoordingsplicht, wat inhoudt dat u moet kunnen aantonen dat uw organisatie in overeenstemming met de AVG handelt. In het verwerkingsregister moet het volgende bijgehouden worden:

- De naam en de contactgegevens van de verwerkingsverantwoordelijke (afdelingshoofd etc.);
- De verwerkingsdoeleinden;
- Een beschrijving van de categorieën van betrokkenen (klanten, medewerkers etc.) en van de categorieën van persoonsgegevens (NAW, betaalgegevens etc.);
- De categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- Informatie over eventuele doorgifte van gegevens naar landen buiten de EU;
- De bewaartermijn van de gegevens;
- De manieren waarop de gegevens zijn beveiligd (encryptie, wachtwoorden etc.)

Een register van verwerkingen is eenvoudig bij te houden met een Excel-sheet, een voorbeeld hiervan is gratis op te vragen bij www.ICTrecht.nl

Technische maatregelen

Zorg ervoor dat u de nodige technologische maatregelen neemt om ervoor te zorgen dat persoonsgegevens zo goed mogelijk beschermd zijn en blijven. Voorbeelden van goede technologische beheersmaatregelen zijn:

- Managed antivirus;
- Managed anti ransomware;
- Geautomatiseerde patches en updates;
- Multi-factor authenticatie;
- Back-up procedures.

KNS Automatisering is gespecialiseerd in het leveren van security oplossingen. U kunt altijd contact opnemen als u advies wilt over passende technologische maatregelen voor het beveiligen van persoonsgegevens.

Organisatorische maatregelen

Zorg ervoor dat u de nodige organisatorische maatregelen neemt om ervoor te zorgen dat persoonsgegevens zo goed mogelijk beschermd zijn en blijven. Voorbeelden van organisatorische maatregelen zijn:

- Gebruikers mogen alleen bij persoonsgegevens die noodzakelijk zijn voor hun werkzaamheden;
- Wachtwoordbeleid (hoofdletters, tekens, letters, periodiek veranderen etc.);
- Zakelijk en privé zaken gescheiden houden (privé mail niet voor zakelijke doeleinde gebruiken etc.).

Analyseer uw situatie met een Data Protection Impact Assessment (DPIA)

Voer een DPIA uit om alle persoonsgegevens verwerkende processen en systemen te analyseren. Denk hierbij aan vragen als:

- Waar staan de persoonsgegevens opgeslagen?
- Welke personen hebben toegang tot deze gegevens?
- Hoe kunnen deze gegevens worden ingezien?
- Voor welke doeleinde gebruiken wij deze gegevens?
- Welke beveiligingsmaatregelen zijn er nu al getroffen?

Op basis van de bevinden uit dit assessment kunt passende technische en/of organisatorische maatregelen nemen om het privacyrisico te verlagen. Een goede methode om de huidige situatie in kaart te brengen is via een workshop of een brainstorm sessie waarbij verschillende medewerkers van verschillende afdelingen aanwezig zijn. De resultaten van dit assessment dienen te worden gedocumenteerd. Het is aan te raden dit assessment periodiek te herhalen.

Privacy by design & privacy by default

Privacy by design houdt in dat u bij het ontwerpen van (nieuwe) diensten of producten er voor zorgt dat persoonsgegevens bij de uitvoering van deze dienst of gebruik van het product goed worden beschermd.

Privacy by default houdt in dat er passende technische en organisatorische maatregelen zijn genomen om ervoor te zorgen dat persoonsgegevens zo goed mogelijk worden beschermd en alleen worden verwerkt als de persoonsgegevens noodzakelijk zijn voor het specifieke doel.

Functionaris Gegevens Bescherming en Privacy Coördinator

Controleer of uw organisatie een Functionaris Gegevens Bescherming nodig heeft. U kunt dit controleren op de website van de Autoriteit Persoonsgegevens.

Het is verstandig om een Privacy Coördinator aan te stellen die verantwoordelijk is voor privacyborging en de effectieve uiting hiervan. Deze persoon zorgt ervoor uw organisatie handelt conform de AVG en is het aanspreekpunt voor de medewerkers voor privacy gerelateerde zaken. Deze persoon is de eindverantwoordelijke voor alle privacy gerelateerde zaken.

Meldplicht datalekken

Alle datalekken moeten worden geregistreerd, gedocumenteerd en direct gemeld bij de Autoriteit Persoonsgegevens. Tevens moet u een interne procedure implementeren voor het afhandelen van datalekken.

Verwerkers-overeenkomsten

Voor alle klanten en leveranciers waarvan u persoonsgegevens verwerkt moeten verwerkersovereenkomsten worden opgesteld en ondertekend door beide partijen. In deze overeenkomst wordt toestemming voor persoonsgegevensverwerking gegeven en worden de details van de verwerking gespecificeerd. Het is aan te raden deze overeenkomsten periodiek te toetsen op relevantie en toereikendheid.

Interne communicatie en training

Er moet een procedure en trainingsprogramma worden opgesteld om er voor te zorgen dat de kennis en bewustwording van medewerkers op het gebied van persoonsgegevensbescherming wordt vergroot c.q. op peil gehouden. Het is aan te raden dit jaarlijks te herhalen.

Jaarplan Privacy

Stel een Jaarplan Privacy op. U kunt op deze manier aantonen dat u actief bezig bent met het naleven van de AVG en zorgt ervoor dat u de ontwikkeling van uw organisatie op het gebied van persoonsgegevensbescherming kan beheersen.

Advies

Als u behoefte heeft aan advies over het voldoen aan de richtlijnen van de AVG dan kunt u altijd contact opnemen via onderstaande contactgegevens.

KNS Automatisering B.V.
Pleimuiden 16 D, 1046 AG Amsterdam
Tel: +31 (0)20-408 09 71
E-mail: info@kns.nl