



DE WEG NAAR DE AVG

JURIDISCH & PRAKTISCH

De Algemene Verordening Gegevensbescherming en uw organisatie

Per 25 mei 2018 dient uw organisatie te voldoen aan de Algemene Verordening Gegevensbescherming (AVG). **Wat betekent dit voor u? Voor uw organisatie? Welke stappen dient u te nemen? Wat zijn de gevolgen bij niet naleving van de AVG?** Kortom: veel vragen en onzekerheden. Met deze factsheet willen wij u een kort overzicht geven van de belangrijkste punten in de AVG en handvatten bieden om binnen uw organisatie mee aan de slag te gaan.



UITGANGSPUNTEN AVG

Het doel van de AVG is om betere bescherming van persoonsgegevens te waarborgen. Onder meer door de rechten van betrokkenen beter te beschermen en voorwaarden te stellen aan de verwerking van persoonsgegevens. Organisaties moeten inzichtelijk maken waarom, waarvoor en op welke wijze persoonsgegevens worden verwerkt. Bij de verwerking dienen de volgende uitgangspunten in acht te worden genomen:

- **Rechtmatig**
- **Behoorlijk**
- **Transparant**
- **Doelbinding** - Het verzameldoel dient welbepaald, gerechtvaardigd en uitdrukkelijk omschreven te zijn.
- **Dataminimalisatie** - De te verwerken persoonsgegevens dienen toereikend, ter zake dienend en noodzakelijk te zijn.
- **Juistheid** - De juistheid van de persoonsgegevens moet worden gewaarborgd door actualisatie en indien nodig rectificatie. Onjuiste persoonsgegevens zorgen voor onrechtmatigheid.
- **Accountability** - De persoonsgegevens worden verwerkt onder verantwoordelijkheid van de (verwerkings)verantwoordelijke die een verantwoordingsplicht heeft.
- **Integriteit en vertrouwelijkheid** - Bij de verwerking van persoonsgegevens dient beveiliging te worden gewaarborgd door het treffen van passende technische en organisatorische maatregelen.
- **Bewaren** - Persoonsgegevens mogen niet langer worden bewaard/opgeslagen dan nodig is voor het verzameldoel en in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor het verzameldoel.

Het doel van de AVG is om betere bescherming van persoonsgegevens te waarborgen.

GRONDSLAGEN VERWERKING PERSOONSGEGEVENS

De verwerking van persoonsgegevens is pas rechtmatig als er sprake is van een van onderstaande grondbeginselen:

- Toestemming betrokkene.
- Noodzakelijk op grond van een overeenkomst.
- Noodzakelijk op grond van wettelijke verplichting verantwoordelijke.
- Bescherming vitale belangen.
- Taak van algemeen belang/uitvoering openbaar gezag.
- Belangenafweging: belang verantwoorde-lijke vs. fundamentele vrijheden betrokkene.

Indien de verwerking niet valt binnen een van bovenstaande grondbeginselen is de verwerking in beginsel onrechtmatig en voldoet daarmee dus niet aan de uitgangspunten van de AVG.

WAT ZIJN PERSOONSGEGEVENS?

Alle gegevens die herleidbaar zijn tot een natuurlijk persoon zoals:

- naam van een persoon
- foto
- NAW-gegevens
- telefoonnummer (ook zakelijk)
- personeelsnummer
- bankrekeningnummer
- kenteken
- audio- of video-opname en soms zelfs postcode en huisnummer

Let op: koppeling van verschillende gegevens kan leiden tot een persoonsgegeven!

WAT VALT ONDER VERWERKING VAN PERSOONSGEGEVENS?

Onder andere:

- | | |
|---------------------------------|----------------|
| ✱ Verzamelen | ✱ Ordenen |
| ✱ Vastleggen | ✱ Structureren |
| ✱ Bijwerken | ✱ Opslaan |
| ✱ Wijzigen | ✱ Wissen |
| ✱ In verband met elkaar brengen | ✱ Vernietigen |
| ✱ Opvragen | ✱ Verspreiden |
| ✱ Raadplegen | ✱ Verstrekken |
| ✱ Gebruiken | ✱ Combineren |
| ✱ Afschermen | |
| ✱ Bewaren | |

RECHTEN BETROKKENE

Betrokkenen krijgen onder de AVG meer rechten ten aanzien van de verwerking van persoonsgegevens.

- Recht op transparante informatie
- Recht van inzage
- Recht op rectificatie en kennisgeving
- Recht op vergetelheid ("right to be forgotten")
- Recht op beperking verwerking
- Recht op overdraagbaarheid gegevens
- Recht van bezwaar
- Recht niet te worden onderworpen aan profilering

WANNEER BENT U VERWERKER/ VERANTWOORDELIJKE?

Verantwoordelijke

- Heeft zeggenschap over het doel en wijze van verwerking;
- Beslist over bezwaartermijnen, verstrekking van gegevens, inzageverzoeken, etc.;
- Is een natuurlijk persoon, rechtspersoon of bestuursorgaan.

Verwerker

- Verwerkt gegevens ten behoeve van verantwoordelijke zonder aan zijn of haar rechtstreeks gezag te zijn onderworpen;
- Staat buiten de organisatie van de verantwoordelijke;
- Neemt geen beslissingen over gebruik, verstrekking aan derden, duur van opslag van gegevens, etc.

CHECKLIST

VERWERKERSOVEREENKOMST

Details met betrekking tot verwerking

- Onderwerp/duur/aard en doel/soort persoonsgegevens.
- Rechten en verplichtingen van verantwoordelijke.

Eisen gesteld aan verwerker

- Verwerking op basis van schriftelijke instructie (o.a. aard/omvang).
- Internationale doorgifte.
- Vertrouwelijkheid gemachtigde personen en opdracht verantwoordelijke.
- Beveiliging.
- Incidenten.
- Subverwerkers inschakelen met toestemming verantwoordelijke.
- Medewerking (o.a. audits, rechten betrokkene, PIA).
- Opslag, verwijdering (o.a. bij einde overeenkomst).

WAAROM EEN PRIVACY IMPACT ASSESSMENT (PIA)?

Een PIA geeft u inzicht in de privacyrisico's van nieuwe of bestaande verwerkingen van persoonsgegevens binnen uw organisatie. Hierdoor kunt u deze risico's vermijden of verminderen.

- Is verplicht als verwerking door aard, omvang, context en doeleinden hoog risico geeft voor betrokkenen.
- Helpt u bij dataminimalisatie.
- Maakt adequate beveiligingsmaatregelen mogelijk/noodzaak duidelijk.
- Draagt bij aan uw verantwoordingsplicht.

WANNEER IS EEN PIA VERPLICHT?

Bij **twee of meer JA's** op onderstaande punten.

1. Beoordelen van mensen op basis van persoonskenmerken (profilieren).
2. Geautomatiseerde beslissingen (uitsluiting/discriminatie).
3. Stelselmatige en grootschalige monitoring (cameratoezicht).
4. Gevoelige gegevens.
5. Grootschalige gegevensverwerkingen (geen definitie: hoeveelheid mensen/gegevens, tijdsduur en geografische reikwijdte).
6. Gekoppelde databases.
7. Gegevens over kwetsbare personen (kinderen, patiënten en schuldsanering).
8. Gebruik van nieuwe technologieën.
9. Doorgifte van persoonsgegevens buiten de EU.
10. Blokkering van een recht, dienst of contract (beoordelen kredietwaardigheid).

VAN MELDPlicht NAAR REGISTRATIEPLICHT

Onder de huidige wetgeving is het verplicht de verwerking van persoonsgegevens te melden bij de Autoriteit Persoonsgegevens. In de AVG is de meldplicht door de registratieplicht vervangen. Deze registratieplicht is niet van toepassing op organisaties met minder dan 250 personen in dienst, tenzij (a) het waarschijnlijk is dat de verwerking een risico inhoudt voor rechten en vrijheden van betrokkenen, (b) de verwerking niet incidenteel is of (c) de verwerking bijzondere categorieën van persoonsgegevens betreft.

Interessant hoe deze uitzonderingen in de praktijk zullen worden uitgelegd.

Immers, iedere organisatie verwerkt persoonsgegevens op structurele basis in de vorm van onder meer een salaris-administratie en klantenbestand.

Waarom een verwerkingsregister?

- Draagt bij aan uw verantwoordingsplicht.
- Belangrijk in het kader van de transparantie.
- Dient als prikkel voor de bewustwording van de verwerkingen binnen de organisatie.
- Maakt het toetsen van de noodzakelijkheid, proportionaliteit en subsidiariteit mogelijk.

PRIVACY BY DESIGN EN DEFAULT

Privacy by design - Al bij het ontwikkelen van producten/diensten dient rekening te worden gehouden met privacy-aspecten. Bijvoorbeeld door Privacy Enhancing Technologies (PET), oftewel privacyverhogende maatregelen.

Privacy by default - De standaardinstellingen bij producten/diensten dienen zo privacy vriendelijk mogelijk te worden ingesteld. Gebruikers kunnen zelf (door een actieve handeling) de mate van privacy bepalen en aanpassen.

DATALEK

Indien u wordt geconfronteerd met een inbreuk in verband met persoonsgegevens waarbij persoonsgegevens verloren zijn gegaan of onrechtmatige verwerking niet valt uit te sluiten, heeft u een meldplicht.

1. De verantwoordelijke meldt uiterlijk 72 uur nadat hij van de inbreuk kennis heeft genomen de gebeurtenis aan de Autoriteit Persoonsgegevens, *“tenzij het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen”*.
2. Een betrokkene dient te worden geïnformeerd indien de inbreuk waarschijnlijk een hoog risico inhoudt voor de persoonlijke levenssfeer.

Deze meldingen hoeven niet te worden verricht indien kan worden aangetoond dat er passende technische en organisatorische maatregelen zijn getroffen (bijvoorbeeld encryptie).

BOETE BIJ OVERTREDING!

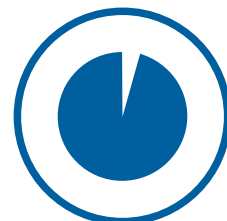
Boetes



tot 20 miljoen



of



4% van wereldwijde jaarlijkse omzet

NIET NALEVING REGELS LEIDT TOT ZWAARDERE SANCTIES:

Geldboete tot € 10 mio of 2% van wereldwijde jaaromzet in voorgaand boekjaar bij bijvoorbeeld (procedureel):

- Ontbreken verwerkersovereenkomst.
- Ontbreken register verwerkingen.

Geldboete tot € 20 mio of 4% van wereldwijde jaaromzet in voorgaand boekjaar bij bijvoorbeeld (materieel):

- Strijdigheid beginselen AVG.
- Rechten van betrokkenen.
- Doorgifte van persoonsgegevens buiten EER.
- Niet naleving bevel AP.

Praktisch



TIPS

1. Creëer awareness binnen uw organisatie.
2. Nulmeting: breng in kaart welke gegevens uw organisatie precies verwerkt.
3. Ga na of u verantwoordelijke en/of verwerker bent.
4. Stel op/update uw verwerkersovereenkomsten.
5. Stel op/update uw privacybeleidsplan en statement! Waarborg de rechten van betrokkenen binnen uw organisatie.
6. Stel op/update uw datalekprotocol. Zorg dat iedereen binnen de organisatie weet wanneer sprake is van een inbreuk en weet hoe te handelen in een dergelijk geval.
7. Ga na wat de grondslag/doel/voor verwerking is en neem dit op in uw privacystatement.
8. Check individuele toegang/rechten van medewerkers en derden.
9. Ga na of u verplicht bent PIA's uit te voeren.
10. Ook indien een PIA niet verplicht blijkt te zijn, adviseren wij een vergelijkbaar instrument binnen uw organisatie te hanteren om zo de risico's omtrent de verwerking te inventariseren en (waar nodig) te verminderen.
11. Documenteer alle door de organisatie te maken en gemaakte stappen op het gebied van privacy.

WAT ZIJN DE (EERSTE) TECHNISCHE STAPPEN OP WEG NAAR DE AVG?

- Maak gebruik van de bestaande encryptie mogelijkheden.
- Gebruik authenticatie techniek.
- Zorg voor loggingdata zodat duidelijk is wie wanneer welke documenten bekijkt.
- Pas document classificatie software toe.
- Gebruik Privacy Enhancing Technologies.
- Geef data een bewaartermijn en registreer deze termijnen.
- Investeer in slimme firewalls.
- Segmenteer uw bedrijfsnetwerk voor Intrusion Detection Systemen.
- Controleer uw netwerk met een Penetration Test en een Vulnerability Scan.

- Maak altijd back-ups en recoveries.
- 90% van alle regels zijn nu ook al van toepassing. Als uw organisatie zaken al op orde heeft, is er niets aan de hand. Anders: vooral achterstallig onderhoud.
- Niet gek laten maken door alle wilde verhalen die er over privacy de ronde doen; begin gewoon.
- Doe het niet omdat boetes kunnen worden opgelegd, maar uit respect voor (de gegevens van) uw klanten of medewerkers. Bovendien: persoonsgegevens zijn het nieuwe goud.
- Doe het niet zelf, maar beleg activiteiten in de organisatie. Maak gebruik van een privacyteam.
- Pak niet alles tegelijk aan maar stel prioriteiten. De inschatting van risico's is hierbij leidend.
- Toon aan dat binnen uw organisatie de wet- en regelgeving wordt nageleefd. Leg alle relevante zaken dus goed vast.
- Besteed tijd aan uw verwerkingenregister. Dit register biedt inzicht in de gegevens die uw organisatie verwerkt en vormt hiermee de basis voor veel van uw privacyactiviteiten.

ONZE AVG ONDERSTEUNING



Privacy Scan

Privacy Scan

Met de Privacy Scan (750 euro) weet u waar u staat en kunt u uw IT-leverancier aan het werk zetten.



Privacy Hotline

Privacy Hotline

Met de Privacy Hotline (500 euro p.m.) helpen wij u snel verder en wijzen u de weg.



Inhouse DPO

Inhouse Data Protection Officer (DPO)

De inhouse DPO van TK is elke week - flexibel - op uw locatie, beantwoordt al uw vragen en geeft direct advies.

Meer informatie?

Voor informatie, advies en begeleiding kunt uw organisatie terecht bij onze gespecialiseerde Privacy- en Arbeidsrechtadvocaten:



Lizette Jaques

T +31 71 535 80 20
M +31 6 458 485 07
E jaques@tk.nl



Rens Goudsmit

T + 31 71 535 80 38
M + 31 6 448 896 14
E goudsmit@tk.nl



Nikki van Steeden

T + 31 71 535 80 20
M + 31 6 148 818 70
E vansteeden@tk.nl



Emiel van der Veen

T + 31 71 535 80 67
M + 31 6 160 116 40
E evanderveen@tk.nl



Debby Boulassel

T + 31 71 535 80 41
M + 31 6 413 988 17
E boulassel@tk.nl



Chris Simonis

T + 31 71 172 419 844
M + 31 6 526 90 564
E simonis@tk.nl