Privacy wetgeving: Wat verandert er in 2018?

Werkgevers verwerken op grote schaal persoonsgegevens van hun werknemers. Vanaf mei 2018 moet elke organisatie voldoen aan de Algemene Verordening Gegevensbescherming (AVG). Deze bevat strengere regels dan de huidige Wbp (Wet bescherming persoonsgegevens). Wat betekent de verandering van Wbp naar AVG voor uw organisatie?

ROBIDUS

ROBIDUS

Inhoud

1. Waarom bescherming van persoonsgegevens?

Digitalisering, toename in het verzamelen en delen van gegevens en technologische ontwikkelingen zorgen voor extra risico's op het gebied van gegevensmisbruik. Persoonsgegevens moeten daarom goed beveiligd worden en iedereen heeft het recht om te weten hoe en waarvoor zijn of haar persoonsgegevens worden gebruikt.

In Nederland wordt dit nu nog geregeld in de Wet bescherming persoonsgegevens. Deze wordt in 2018 vervangen door de AVG: de Algemene Verordening Gegevensbescherming.

1.1 Waarom wordt de Wbp vervangen door de AVG?

De Wet bescherming persoonsgegevens stamt uit 2000 en is gebaseerd op een privacyrichtlijn uit 1995. Diverse technologische ontwikkelingen en mogelijkheden hebben ervoor gezorgd, dat de oude privacywetgeving niet meer voldoet. Denk alleen al aan de groei van professionele cybercriminaliteit. Tevens wordt het nu belangrijker gevonden dat elke Europese burger dezelfde bescherming krijgt. Als de AVG van toepassing is, geldt er nog maar één privacywet in de hele Europese Unie (EU) in plaats van 28 verschillende nationale wetten. In Nederland zullen enkele regels met betrekking tot de uitvoering worden vastgesteld in de Uitvoeringswet AVG.

1.2 Om welke persoonsgegevens gaat het?

De meest gebruikte persoonsgegevens zijn iemands naam, adres en woonplaats. Ook vallen bijvoorbeeld telefoonnummers en e-mailadressen onder 'persoonsgegevens'. Eigenlijk alle data die te herleiden zijn naar een natuurlijk persoon. Daarnaast zijn er persoonsgegevens die als (zeer) gevoelig kunnen worden bestempeld, zoals iemands ras, godsdienst of gezondheid. Dit worden bijzondere persoonsgegevens genoemd en kennen de meest strenge beveiligingseisen.

2. Wat zijn de belangrijkste onderwerpen in de AVG?

Per 25 mei 2018 gaan in het kort de volgende punten veranderen op het gebied van privacywetgeving:

- versterking en uitbreiding van privacyrechten;
- meer verantwoordelijkheden voor bedrijven;
- dezelfde bevoegdheden voor alle Europese privacy toezichthouders (in Nederland is dit de Autoriteit Persoonsgegevens), zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.

2.1 Belangrijke regels van de AVG

De AVG bevat regels waarmee de persoonsgegevens van elke Europese burger op dezelfde manier worden beschermd. De belangrijkste hiervan zijn:

Eigen verantwoordelijkheid

Werkgevers moeten kunnen aantonen dat zij de juiste technische en organisatorische maatregelen hebben getroffen om aan de AVG-eisen te voldoen.

Controleur aanstellen

Bepaalde organisaties zijn verplicht een Data Protection Officer (DPO) of Functionaris voor Gegevensbescherming (FG) aan te stellen. Dat hoeft niet per se een werknemer van de betreffende organisatie te zijn.

Boetes

Houdt u zich niet aan de regels? Dan kan een boete van maximaal 20 miljoen euro (of 4 procent van de totale omzet) worden opgelegd.

Rechten van betrokkenen

De rechten van betrokkenen zijn in de AVG aangescherpt. U dient te kunnen voldoen aan verzoeken met betrekking tot:

- Het recht op inzage;
- Het recht op vergetelheid en verwijderen van gegevens;
- Het recht op dataportibiliteit;
- Het recht om de verwerking te beperken;
- Het recht om bezwaar te maken tegen het verwerken van gegevens.

3. Wat zijn de belangrijkste onderwerpen in de AVG?

Meldplicht datalekken

Sinds 1 januari 2016 bestaat de meldplicht datalekken. Deze is opgenomen in de Wbp en zal ook van toepassing zijn bij de Algemene Verordening Gegevensbescherming. De AVG stelt dat de verwerkingsverantwoordelijke een 'inbreuk in verband met persoonsgegevens' (datalek) binnen 72 uur na constatering dient te melden aan de Autoriteit Persoonsgegevens. Het niet voldoen aan de meldplicht kan leiden tot boetes.

Verwerkingsvoorwaarden

De AVG heeft verwerkingsvoorwaarden, waaraan alle verwerkingen van persoonsgegevens moeten voldoen:

- Persoonsgegevens moeten op juiste, rechtmatige en transparante manier worden opgeslagen;
- Persoonsgegevens mogen alleen voor een bepaald uitdrukkelijk beschreven doel worden opgeslagen;
- Alleen persoonsgegevens die noodzakelijk zijn voor het doel mogen worden opgeslagen;
- Gegevens moeten juist en actueel zijn;
- Als identificatie niet meer noodzakelijk is voor het doel, dan moeten de persoonsgegevens worden verwijderd of geanonimiseerd;
- De persoonsgegevens moeten worden beveiligd door middel van technische en organisatorische maatregelen.

Documentatieplicht

Elk bedrijf moet kunnen aantonen dat de regels van de AVG opgevolgd worden. Denk hierbij aan de administratie van de toestemming, alle gegeven informatie, rechten van betrokkenen, minimalisatie van verwerking van persoonsgegevens en afspraken met administratieve medewerkers. Zowel de verwerkingsverantwoordelijke als de verwerker dienen registers van verwerkingsactiviteiten bij te houden.

Overeenkomst met verwerker

Verwerkingsverantwoordelijke en verwerker zijn verplicht afspraken ten aanzien van de verwerking vast te leggen in een verwerkersovereenkomst. Hierin moeten ten minste de volgende onderwerpen worden beschreven:

- Het doel van de verwerking;
- Het soort persoonsgegevens dat wordt verwerkt;
- De categorieën van personen wiens gegevens worden opgeslagen;
- Dat passende beveiligingsmaatregelen zullen worden genomen;
- Dat de verwerker meewerkt aan audits om te controleren of de verwerker zich aan alle verplichtingen houdt en na afloop van de verwerking de persoonsgegevens vernietigt of retourneert;

- De verwerker mag geen derde partij inschakelen zonder voorafgaand schriftelijke toestemming te verkrijgen van het bedrijf of de persoon van wie gegevens worden opgeslagen.

Privacy by design, Privacy by default en PIA
Privacy moet uitgangspunt zijn bij het ontwikkelen van nieuwe systemen, processen en dienstverleningen. De principes van Privacy by design/default vormen hierbij een belangrijke basis. Daarnaast stelt de AVG verwerkingsverantwoordelijken verplicht om bij verwerking die mogelijk een hoog risico met zich meebrengt een Privacy Impact Assessment (in de AVG 'gegevensbeschermingseffectbeoordeling') uit te voeren.

3.1 Wanneer mag u persoonsgegevens (niet) verwerken?

Er zijn een aantal voorwaarden die bepalend zijn voor de rechtmatigheid van de verwerking. U mag persoonsgegevens verwerken wanneer aan tenminste één van deze punten wordt voldaan:

- **Wanneer de betrokkene toestemming heeft gegeven om zijn gegevens te laten verwerken**: hierbij dient elke twijfel te zijn uitgesloten over de vraag of deze persoon zijn toestemming heeft gegeven. Bij meerdere verwerkingen van persoonsgegevens moet er bij alle verwerkingen apart toestemming worden gegeven.
- **Bij het opstellen of uitvoeren van een overeenkomst:** wanneer de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst.
- **Bij een wettelijke verplichting:** wanneer de gegevensverwerking noodzakelijk is om te voldoen aan een wettelijke verplichting van de verantwoordelijke partij, zoals bij het invullen van belastingpapieren.
- **Bij gezondheidsbelangen:** wanneer de gegevensverwerking noodzakelijk is om de gezondheidsbelangen van de betrokkene te beschermen. Bijvoorbeeld wanneer een Eerste Hulp-arts een behandelovereenkomst moet sluiten op basis van medische gegevens van de betrokkene.
- **Algemeen belang:** wanneer de verwerking noodzakelijk is voor bijvoorbeeld een publieksrechtelijke taak, zoals de uitoefening van het openbaar gezag (politie).

4. De rol van Robidus

Robidus verwerkt persoonsgegevens in opdracht van honderden werkgevers. Om te voldoen aan de privacyrichtlijnen heeft Robidus technische en organisatorische maatregelen genomen die ook de opdrachtgever in acht dient te nemen.

Verwerkersovereenkomst

Voorafgaand aan de dienstverlening wordt tussen opdrachtgever en Robidus een verwerkersovereenkomst opgesteld. Deze geeft de rechten en verplichtingen van beide partijen weer waar het de bescherming van de persoonsgegevens van opdrachtgever betreft.

Beveiligde informatie-uitwisseling

Voor het uitvoeren van onze dienstverlening hebben we gegevens van onze opdrachtgevers nodig en kan het noodzakelijk zijn om gegevens te delen met andere partijen (verzekeraars, UWV, bedrijfsartsen). De uitwisseling van die data vindt altijd beveiligd plaats. Dit kan zijn door informatie direct te verwerken in onze software HRControlNet, beveiligde koppelingen met andere applicaties of door gebruik te maken van beveiligde informatie-uitwisseling via FileCap.

ISO 27001 certificering

De fysieke en logische toegangsbeveiliging tot onze informatiesystemen voldoen aan de internationale ISO 27001standaard. Naast een integriteitscheck van ons personeel hebben we strenge technische en organisatorische maatregelen getroffen om vertrouwelijke gegevens correct te kunnen verwerken. Alle getroffen beveiligingsmaatregelen worden continu gemonitord door onze Compliance Officer.