TIPS OM UW ORGANISATIE VOOR TE BEREIDEN OP DE NIEUWE PRIVACYREGELS

Zet u schrap voor de nieuwe privacyregels

Vanaf 28 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Alhoewel 2018 nog ver weg lijkt, zal deze verordening een zeer grote (financiële) impact hebben op uw organisatie. Vanaf dat moment is er namelijk nog maar één privacywet die in de gehele EU geldt en vervalt de Wet bescherming persoonsgegevens (WBP). Hoe bereidt uw organisatie zich voor op de nieuwe privacywetgeving?

Op dit moment heeft elke lidstaat binnen de EU nog een eigen privacywet. Deze privacywetten zijn wel allemaal gebaseerd op de Europese privacyrichtlijn uit 1995. In Nederland is de nationale uitvoering van deze richtlijn de Wet bescherming persoonsgegevens (WBP). De Europese privacyrichtlijn was verouderd. Zo heeft het internet de afgelopen jaren een enorme ontwikkeling doorgemaakt. Dit maakte het nodig om de Europese privacywetgeving te herzien. Het resultaat is de Algemene Verordening Gegevensbescherming (AVG).Hoewel de AVG pas op 28 mei 2018 van toepassing is, is deze verordening al op 28 mei 2016 in werking getreden. Dit betekent dat uw organisatie twee jaar de tijd heeft gekregen om zich op deze verordening voor te bereiden (in de tussentijd blijft de WBP gelden). Gebruik deze tijd om de volgende punten te overwegen.

1. Registratieplicht

Vanaf 28 mei 2018 zijn organisaties met meer dan 250 werknemers verplicht om met onderliggende documentatie aan te tonen dat zij correcte maatregelen hebben genomen om aan de AVG te voldoen. Deze verplichting wordt ook wel de registratieplicht genoemd. Voor kleinere organisaties geldt deze registratieplicht niet, tenzij er sprake is van risicovolle of structurele verwerkingen dan wel verwerkingen met bijzondere personeelsgegevens, zoals gezondheidsgegevens. De registratieplicht schrijft voor dat u een overzicht moet opstellen waarin u alle verwerkingen van persoonsgegevens inzichtelijk maakt en bijhoudt (inclusief het doel, de grondslag en de beveiligingsmaatregelen). Tegenover deze registratieplicht staat dat u niet langer verplicht bent om verwerkingen van persoonsgegevens te melden bij de Autoriteit Persoonsgegevens.

Actief in meerdere landen

De AVG is een verordening. Dit houdt in dat de regels die hierin staan rechtstreekse werking hebben. Is uw organisatie in meerdere EU-landen actief, dan heeft dit als voordeel dat u in al deze verschillende landen te maken heeft met dezelfde privacyregels. Daarnaast heeft u straks nog maar te maken met één privacytoezichthouder (de zogeheten leidende toezichthouder). Dit is de toezichthouder van het EU-land waar de hoofdvestiging van uw organisatie gevestigd is.

2. Functionaris voor gegevensbescherming

Controleer of het noodzakelijk is om een functionaris voor gegevensbescherming aan te stellen. Hiertoe is uw organisatie onder meer verplicht als u op grootschalige wijze bijzondere persoonsgegevens verwerkt. Denk bijvoorbeeld aan een ziekenhuis dat veelvuldig patiëntgegevens verwerkt. De functionaris moet een natuurlijk persoon zijn. Het is dus niet mogelijk om bijvoorbeeld een commissie of (compliance)afdeling aan te wijzen. Om de functionaris zijn taak goed te kunnen laten uitvoeren, is onder meer het volgende van belang:

- actieve steun vanuit de directie en het management;
- voldoende tijd en ruimte om de taken naar behoren uit te voeren;
- voldoende budget, faciliteiten en persoonele ondersteuning;
- duidelijke interne communicatie over de benoeming;
- het bieden van scholing.

Om de onafhankelijkheid van de functionaris te waarborgen, mag hij geen instructies krijgen over de wijze waarop hij zijn taak uitvoert. Daarnaast kunt u een functionaris niet ontslaan als gevolg van de uitoefening van zijn functionaristaken. Tot slot moet u belangenverstren-

geling met de overige taken die de functionaris vervult, proberen te voorkomen.

3. Privacy bij design

Op grond van de AVG moet alle software die uw organisatie gebruikt om persoonsgegevens te verwerken voldoen aan het 'privacy by design'-vereiste. Dit betekent dat er bij het ontwerpen van een informatiesysteem al rekening wordt gehouden met privacy en het zo min mogelijk verwerken van persoonsgegevens. Het doel van 'privacy by design' is dat de beveiliging van persoonsgegevens wordt geoptimaliseerd. Het advies is dus om alle software die in uw organisatie wordt gebruikt om persoonsgegevens op te slaan en te verwerken tegen het licht te houden. Als u bijvoorbeeld persoonsgegevens opslaat in Excel, Word of andere software die hiervoor niet is bedoeld, zult u mogelijk naar alternatieven moeten kijken. Overigens is het nog de vraag of het beveiligen van een Excel- of Word-document met een wachtwoord afdoende is om aan het privacyvereiste te voldoen. De rechtspraak zal dit in de toekomst moeten uitkristalliseren.

4. Toestemming

Als uw organisatie niet kan aantonen dat een verwerking van persoonsgegevens strikt noodzakelijk is, zult u hiervoor expliciet om toestemming moeten vragen aan uw werknemers. Denk aan een smoelenboek op intranet waarin u een foto van een werknemer wilt plaatsen.

Hoewel het toestemmingsvereiste in de huidige Wet bescherming persoonsgegevens ook is opgenomen, gaat de Europese privacyverordening bij de invulling van het begrip toestemming een stuk verder:

- Er is een actieve handeling van de werknemer vereist om zijn toestemming openbaar te maken.
- Er moet sprake zijn van ondubbelzinnige toestemming.
- De toestemming moet vrijwillig gegeven zijn (zie kader onderaan).
- De werknemer moet weten voor welke gegevensverwerking en voor welk doel hij toestemming geeft.
- Een werknemer moet in duidelijke en eenvoudige taal worden geïnformeerd.

Uw organisatie moet bewijzen dat u geldige toestemming van uw werknemers heeft gekregen voor de verwerking van persoonsgegevens. Het moet voor werknemers bovendien mogelijk zijn om hun toestemming in te trekken en u moet uw werknemers hierover ook informeren. Het intrekken van de toestemming moet bovendien net zo eenvoudig zijn als het geven van de toestemming. Zorg er dus voor dat u uw HR-beleid hierop aanpast.

5. Datalek

Net als de WBP kent de AVG een meldingsplicht bij datalekken. Van een datalek is volgens de AVG sprake bij iedere inbreuk op de beveiliging van persoonsgegevens die leidt tot ongeoorloofde verwerking (zoals verlies en vernietiging) daarvan. Als de systemen van uw organisatie bijvoorbeeld zijn gehackt waardoor de hacker toegang heeft gekregen tot gevoelige persoonsgegevens of een USB-stick met diverse cv's van sollicitanten is gestolen, zult u hiervan binnen 72 uur melding moeten doen bij de Autoriteit Persoonsgegevens. Afhankelijk van de omstandigheden, moet u het datalek ook melden aan de personen van wie de persoonsgegevens zijn gelekt. Zorg dat u een procedure opstelt waarin u duidelijk in kaart brengt welke stappen uw organisatie moet nemen als u te maken krijgt met een mogelijk datalek.

Wanneer is er sprake van vrijwillige toestemming?

Bij het bestaan van een gezagsverhouding, zoals de relatie tussen werkgever en werknemer, kan de vraag bestaan of er wel sprake is van vrijelijke toestemming voor het verwerken van persoonsgegevens. Om in zijn eigen levensonderhoud te kunnen voorzien, is een werknemer doorgaans immers afhankelijk van het salaris dat hij ontvangt van zijn werkgever. Hierdoor kan hij toestemming geven voor een bepaalde verwerking omdat hij zich onder druk gezet voelt. Gelet hierop heeft het in een werkgever-werknemerrelatie de voorkeur om de grondslag van de verwerking op een andere grondslag dan toestemming te baseren.

Andere grondslag

Zo'n andere grondslag kan bijvoorbeeld een wettelijke verplichting zijn. Zo is uw organisatie verplicht om gegevens over uw werknemers aan de Belastingdienst te verstrekken. In zo'n geval hoeft u dus geen toestemming te vragen.

Om toestemming vragen bij indiensttreding?

Het is af te raden om werknemers bij indiensttreding al in zijn algemeenheid om toestemming te vragen voor verwerkingen van persoonsgegevens. Soms staat er een generieke toestemmingsbepaling in een arbeidsovereenkomst die dit moet regelen. Dit heeft weinig waarde omdat u op grond van de privacyregels heel specifiek moet aangeven voor welke verwerking u toestemming vraagt en met welk doel u dit doet.

Boeterisico

Als u niet op een juiste manier omgaat met het verwerken van persoonsgegevens op grond van de AVG, loopt uw organisatie een aanzienlijk boeterisico. Sinds 1 januari 2016 heeft de Autoriteit Persoonsgegevens namelijk veel meer boetebevoegdheden gekregen en dit wordt nog verder uitgebreid. Er kunnen vanaf mei 2018 boetes tot € 20 miljoen of 4% van de wereldwijde jaaromzet (!) worden opgelegd aan organisaties. Daarnaast wordt de drempel om een boete op te leggen verlaagd. Niet langer is opzet of ernstig verwijtbare nalatigheid vereist om direct een boete op te leggen.

Naomi Giling, arbeidsrechtadvocaat bij L&A advocaten te Amsterdam, e-mail: naomi.giling@LenAadvocaten.nl, www.LenAadvocaten.nl