AVG: 'The day after'

De Autoriteit Persoonsgegevens heeft op 6 juni 2018 aangegeven dat zij 25 tot 30 klachten per dag ontvangt over toepassing van de AVG in diverse organisaties. Hoewel minister Dekker heeft aangegeven dat kleine Nederlandse organisaties aanvankelijk minder streng zullen worden getoetst, is het toch belangrijk om te zorgen dat een organisatie AVG-proof is.
Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van kracht geworden. Sindsdien geldt in de EU één privacywet. Nog lang niet alle organisaties en bedrijven blijken AVG-proof te zijn. Speciaal voor de HR-professional hierbij vier aandachtspunten:

1. Controleer of de verwerkingen van persoonsgegevens die bij HR plaatsvinden kunnen worden gebaseerd op een grondslag die de AVG noemt
Een werkgever mag persoonsgegevens van werknemers verwerken wanneer dit nodig is ter voorbereiding of uitvoering van de arbeidsovereenkomst, wanneer dit nodig is om aan een wettelijke verplichting te voldoen of wanneer hiervoor een gerechtvaardigd belang bestaat (denk aan screening). Indien de verwerking niet kan worden gebaseerd op een dergelijke grondslag dient expliciete toestemming van de werknemer te worden verkregen. Omdat ervan uitgegaan moet worden dat een werknemer zijn toestemming veelal niet vrijelijk kan verlenen, dient de toestemmingsgrondslag in de arbeidsrelatie terughoudend te worden gebruikt.

2. Let op bewaartermijnen en vernietiging van persoonsgegevens
Wanneer de gegevens niet meer nodig zijn voor het doel waarvoor ze zijn verzameld of worden gebruikt, dienen de gegevens vernietigd te worden, tenzij er nog een wettelijke bewaartermijn geldt. Een concrete bewaartermijn geeft de AVG niet. Over het algemeen dienen gegevens in de personeelsdossiers 2 jaar na het einde van het dienstverband te worden vernietigd, maar er geldt een wettelijke bewaartermijn van 7 jaar voor bepaalde fiscaal relevante salarisadministratie en 5 jaar voor een kopie ID. Ook hebben werkgevers die eigenrisicodrager zijn voor de ZW of de WGA een belang om re-integratiedossiers langer te bewaren (respectievelijk 5 en 10 jaar). Vernietig bepaalde documenten uit de personeelsdossiers dus tijdig, maar zeker ook niet te vroeg.

3. Zorg dat de HR-afdeling de rechten van werknemers kan uitvoeren
Werknemers hebben diverse rechten, zoals het recht op inzage, rectificatie en/of het laten verwijderen van persoonsgegevens. Ook hebben werknemers recht op informatie over de verwerkingen. In dat kader dient aan werknemers een informatiebrief/privacyverklaring te worden verstrekt en moet voldaan kunnen worden aan het recht op inzage in het personeelsdossier.

4. Stel een protocol datalekken op
Wanneer er sprake is van een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan of onrechtmatige verwerking niet is uit te sluiten, is er een datalek. Voorbeelden zijn een vergeten laptop, een kwijtgeraakte smartphone of een e-mail met alle ontvangers in de cc in plaats van de bcc. Een werkgever moet een datalek intern registreren en in sommige gevallen melden bij de Autoriteit Persoonsgegevens en/of de betrokkenen. Omdat een melding al binnen 72 uur moet worden gedaan, is het van belang dat medewerkers weten wanneer er een datalek is en wat zij dan moeten doen. Een protocol datalekken in de organisatie zal eraan bijdragen dat er voortvarend kan worden gehandeld bij een datalek.

Marjolein Gobes *is advocaat arbeidsrecht bij Van Diepen Van der Kroef Advocaten. Ook is zij docent van het seminar 'Privacy op de werkvloer: de impact van de AVG op HR'. www.hracademy.nl*