AUTORITEIT
PERSOONSGEGEVENS

Het OR-privacyboekje

De rol van de ondernemingsraad bij privacy op de werkvloer

Inhoudsopgave

AUTORITEIT
PERSOONSGEGEVENS

1. Inleiding: privacy en de ondernemingsraad

Personeelsdossiers. Registratie van ziekteverzuim. Camera's op de werkplek. Screening van personeel. Werkgevers verwerken veel persoonsgegevens van hun werknemers. En sommige van die verwerkingen kunnen heel ingrijpend zijn. Het is daarom uiterst belangrijk dat werkgevers rekening houden met de privacy van hun werknemers. En dat hierover wordt gesproken binnen de organisatie. Daarbij spelen ondernemingsraden een cruciale rol. De ondernemingsraad (OR) is nauw betrokken bij afspraken over de verwerking van persoonsgegevens van personeel en bij personeelsvolgsystemen.

De Wet op de Ondernemingsraden (WOR) bepaalt dat de werkgever de OR moet vragen om in te stemmen met regelingen waarvoor persoonsgegevens van werknemers worden verwerkt. De werkgever moet de OR om een oordeel vragen bij (tekst uit de wet):

1. Een regeling omtrent het verwerken alsmede de bescherming van persoonsgegevens van de personen die in de onderneming werkzaam zijn (geregeld in artikel 27, eerste lid onder k. van de WOR).
2. Regelingen inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de personen die in de onderneming werkzaam zijn (ofwel personeelsvolgsystemen; geregeld in artikel 27, eerste lid onder l. van de WOR).

De OR is dus medeverantwoordelijk voor de omgang met en de bescherming van persoonsgegevens op het werk. Om ondernemingsraden ondersteuning te bieden bij de afwegingen die zij daarbij moeten maken, heeft de Autoriteit Persoonsgegevens (AP) deze handreiking ontwikkeld.[1]

De handreiking begint met een korte vragenlijst die u helpt te begrijpen wat precies wordt verstaan onder een 'regeling omtrent het verwerken van persoonsgegevens'. Daarna volgt een schets van de privacyregels uit de Algemene verordening gegevensbescherming (AVG). Hier vindt u ook voorbeelden en suggesties voor vragen die u als OR kunt stellen wanneer u een regeling of voorziening als bedoeld in de WOR aan de AVG toetst.

Zeker als een werkgever overweegt personeelsvolgsystemen in te zetten, moet hij de OR daarbij betrekken. De handreiking sluit daarom af met toetsingsvragen speciaal voor dit type verwerkingen.

In deze handreiking hanteren we de begrippen 'werkgever' en 'werknemer'. Het begrip 'werkgever' sluit aan bij het in artikel 1, eerste lid onder d. van de WOR gedefinieerde begrip 'ondernemer': 'de natuurlijke persoon of de rechtspersoon die een onderneming in stand houdt'. Met het begrip 'werknemer(s)' bedoelen we de in de onderneming werkzame persoon of personen in de zin van artikel 2 van de WOR ('medewerker(s)').

De WOR is van toepassing op zowel het bedrijfsleven als de overheid.

Om de inhoud van deze handreiking zo begrijpelijk mogelijk te maken, staat in groene kaders een voorbeeld beschreven van een werkgever die gps-trackers wil inzetten. Dit voorbeeld komt op verschillende plekken in de handreiking terug om de privacyregels uit de AVG concreter te maken.

[1] Deze handreiking vervangt de oude handreiking 'Privacy: Checklist voor de ondernemingsraad'.

2. Het instemmingsrecht van de OR

De WOR geeft de OR instemmingsrecht bij een voorgenomen besluit over een regeling voor het verwerken van persoonsgegevens van werknemers. Maar wat is een persoonsgegeven precies? En wat verstaan we onder verwerken? Dat moet u weten om te kunnen bepalen of het instemmingsrecht van toepassing is. Voor de interpretatie van de begrippen 'persoonsgegevens' en 'verwerking' kijken we naar de AVG.

Is er sprake van een persoonsgegeven?
Een persoonsgegeven in de zin van de AVG is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (de 'betrokkene' genoemd). Het kan om allerlei soorten informatie gaan: niet alleen om voor de hand liggende gegevens als iemands naam, adres en telefoonnummer, maar ook om eigenschappen van deze persoon, opvattingen of gedrag.

Voorbeelden van persoonsgegevens zijn:

- naam, adres, burgerservicenummer;
- een video-opname van een persoon;
- gegevens over iemands telefoon- of computergebruik;
- het kentekennummer van een auto.

Van een persoonsgegeven is pas sprake als de identiteit van de persoon over wie de informatie gaat ook redelijkerwijs kan worden vastgesteld. Dat kan direct, maar ook indirect: bijvoorbeeld wanneer door het combineren van verschillende gegevens over een persoon kan worden afgeleid om wie het gaat. De informatie moet individualiseerbaar zijn. Of gegevens individualiseerbaar zijn, hangt af van wat redelijkerwijs binnen de mogelijkheden van de onderneming ligt. Of wat de onderneming met aanvullende informatie kan achterhalen.

Werkgever X wil meer grip krijgen op het gebruik van de (zakelijke) wagens in zijn wagenpark. Zijn werknemers gebruiken de wagens om klanten te bezoeken. Werkgever X wil een gps-tracker in de wagens laten plaatsen. Zo kan werkgever X nagaan welke werknemer zich het dichtst bij een klant bevindt en gedurende de dag de optimale route voor zijn wagens inplannen. Enkele werknemers rijden de zakelijke wagens ook privé. Werkgever X wil de gps-tracker daarom ook inzetten om in de kilometerregistratie onderscheid te maken tussen werk- en privékilometers.

Een gps-tracker verzamelt locatiegegevens. Werkgever X weet welk gps-signaal bij welke wagen hoort en welke werknemer de bestuurder van deze wagen is. Het is daarom duidelijk dat de locatiegegevens persoonsgegevens zijn.

Zodra gegevens tot een werknemer te herleiden zijn, is al snel sprake van persoonsgegevens. Een personeelsnummer in een bedrijf is tot een persoon te herleiden. Ook met een persoonlijke loginnaam is een werknemer te traceren.

Geen persoonsgegevens zijn bijvoorbeeld:

- gegevens over het telefoongebruik binnen de organisatie die niet tot individuele werknemers te herleiden zijn;
- gegevens die tot een geheel zijn samengevoegd ('geaggregeerde gegevens') over het personeelsbestand van een bedrijf met een redelijke omvang.

Let op! Naast 'gewone' persoonsgegevens kent de AVG ook zogeheten bijzondere persoonsgegevens. Dat zijn persoonsgegevens die door hun aard bijzonder gevoelig zijn. Deze persoonsgegevens krijgen extra bescherming in de AVG.

Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens waaruit iemands ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of lidmaatschap van een vakbond blijken. Daarnaast kan het gaan om genetische gegevens, biometrische gegevens (gebruikt om iemand te identificeren), gegevens over iemands gezondheid of gegevens over iemands seksueel gedrag of seksuele gerichtheid.

Voorbeelden van bijzondere persoonsgegevens op het werk zijn:

- gegevens over ziekteverzuim;
- gegevens over alcohol-, medicijn- of drugsgebruik;
- gegevens over lidmaatschap van een vakbond of politieke partij;
- een irisscan, vingerafdruk of gezichtsscan (biometrische gegevens).

De verwerking van bijzondere persoonsgegevens is verboden, tenzij de onderneming zich kan beroepen op een wettelijke uitzondering (zoals genoemd in artikel 9 lid 2 AVG).

De bedrijfswagens van werkgever X worden door sommige werknemers ook privé gebruikt. Deze werknemers maken zich zorgen om wat de gps-tracker registreert buiten werktijd. Uit locatiegegevens kunnen namelijk gevoelige privégegevens worden afgeleid.

Bijvoorbeeld wanneer de werknemer met de auto een kerk bezoekt of naar een medische afspraak gaat. Zo kunnen er (onbedoeld) bijzondere persoonsgegevens worden verzameld van werknemers. Heeft werkgever X nagedacht over een mogelijkheid om de gps-tracker stop te zetten als een werknemer pauzeert of de wagen in privétijd gebruikt?

Medische gegevens zijn niet alleen bijzondere persoonsgegevens, maar vallen ook onder het medisch beroepsgeheim. Daarom is het van groot belang dat de werkgever deze gegevens niet beheert, maar dat bijvoorbeeld de bedrijfsarts dat doet.

Is er sprake van een verwerking van persoonsgegevens?
De AVG kent het ruime begrip 'verwerking van persoonsgegevens.' Hieronder wordt verstaan: een bewerking (of een geheel van bewerkingen) van persoonsgegevens (of een geheel van persoonsgegevens), al dan niet uitgevoerd via geautomatiseerde procedés. Bijvoorbeeld: gegevens verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, doorsturen, verspreiden, combineren, afschermen, wissen of vernietigen.

De gps-tracker stuurt de locatiegegevens door naar werkgever X. Die kan de werknemers niet alleen live volgen, maar kan ook terugzoeken welke routes zijn afgelegd. Hier is onder meer sprake van gegevens verzamelen, vastleggen, opslaan en gebruiken: allemaal verwerkingen van persoonsgegevens.

Wie is de verwerkingsverantwoordelijke?
Zodra ergens persoonsgegevens worden verwerkt, is er altijd een zogeheten verwerkingsverantwoordelijke. Dat is degene die beslist of er persoonsgegevens worden verwerkt, en zo ja, welke gegevens, met welk doel en op welke manier.

Om te bepalen wie de verwerkingsverantwoordelijke is, is niet alleen de formeel-juridische zeggenschap van belang, maar ook de feitelijke invloed die de werkgever uitoefent op de verwerking.

In de WOR is geregeld wat onder een 'onderneming', 'ondernemer' en 'bestuurder' moet worden verstaan. Over het algemeen is de werkgever (de ondernemer in de zin van de WOR) de verwerkingsverantwoordelijke bij de verwerking van personeelsgegevens.

Werkgever X wil de gps-tracker gebruiken om werknemers naar de dichtstbijzijnde klanten te sturen en om de kilometerregistratie te controleren. Werkgever X bepaalt het doel en de middelen van de verwerking van de locatiegegevens en is dus verwerkingsverantwoordelijke.

Verwerkt de werkgever niet zelf persoonsgegevens, maar laat deze de feitelijke handelingen verrichten door een daarin gespecialiseerde organisatie? Dan is deze organisatie een zogeheten verwerker. De verwerkingsverantwoordelijke blijft ook verantwoordelijk voor de verwerkingen die worden uitbesteed.

De AVG schrijft voor dat de verwerkingsverantwoordelijke en de verwerker afspraken maken over de verwerking. Dat doen zij in een verwerkersovereenkomst. Hierin staan afspraken over de precieze opdracht van de verwerking, wat de verwerker wel en niet met de persoonsgegevens mag doen en welke waarborgen worden getroffen om gegevens te beveiligen. De verwerker mag de persoonsgegevens niet voor andere (eigen) doeleinden gebruiken.

Ook spreken de verwerker en de verwerkingsverantwoordelijke af dat de verwerker de persoonsgegevens verwijdert na afloop van de verwerkingsdiensten. Of dat de persoonsgegevens terug worden gegeven aan de verwerkingsverantwoordelijke.

In de praktijk kan het lastig zijn om te bepalen of een organisatie verwerker of verwerkingsverantwoordelijke is. Een paar voorbeelden van verwerkers die uw onderneming wellicht inzet om persoonsgegevens van werknemers te verwerken:

- Salarisadministratiebureaus: geeft de werkgever duidelijke instructies over wie er betaald moet worden, op welke datum en hoe lang de gegevens bewaard moeten blijven? Dan vindt de verwerking van persoonsgegevens plaats in opdracht van de werkgever. Het salarisadministratiebureau mag als verwerker de persoonsgegevens niet voor eigen doeleinden gebruiken.
- IT-dienstverlener: schakelt de werkgever een IT-dienstverlener in om de IT-systemen van de organisatie te beheren? Dan is het vaak onvermijdelijk dat de IT-dienstverlener systematisch toegang heeft tot persoonlijke gegevens van werknemers. Hoewel de toegang tot deze persoonsgegevens niet het hoofddoel is van de ondersteunende dienstverlening, moet de werkgever als verwerkingsverantwoordelijke afspraken maken met deze verwerker.

Verwerkt de andere organisatie de door de werkgever verstrekte persoonsgegevens voor eigen, zelf bepaalde doeleinden? Dan is deze organisatie ook verwerkingsverantwoordelijke en is er sprake van gezamenlijke verwerkingsverantwoordelijkheid.

Voor meer informatie, zie dossier Verwerkers op de website van de AP.

Werkgever X overweegt om de locatiegegevens die de gps-tracker verzamelt te laten analyseren door een gespecialiseerd bedrijf, zodat werkgever X het wagenpark zo efficiënt mogelijk kan inzetten. Ook het analyseren van de locatiegegevens is een verwerking van persoonsgegevens. Werkgever X is ook voor deze verwerking verwerkingsverantwoordelijke. Het gespecialiseerde bedrijf dat de opdracht krijgt voor de analyse, is waarschijnlijk een verwerker.

Moet de OR om instemming worden gevraagd?
Heeft de werkgever het voornemen een regeling te treffen voor de verwerking van persoonsgegevens van personeel of een personeelsvolgsysteem? Dan moet de werkgever dit ter instemming aan de OR voorleggen. Ook het wijzigen of intrekken van een bestaande regeling valt hieronder.

Regelingen voor het verwerken van personeelsgegevens komen in vrijwel elke organisatie voor. Zo heeft de OR bijvoorbeeld instemmingsrecht bij regelingen over personeelsdossiers, verzuimregistratie en de salarisadministratie.

Ook personeelsvolgsystemen komen veel voor. Een personeelsvolgsysteem is een systeem dat gericht is op – of geschikt is voor – waarneming van werknemers of controle van hun aanwezigheid, gedrag of prestaties. Gebruikt een werkgever een bepaald systeem hier niet voor, maar zou dit wel kunnen? Ook dan is dit een personeelsvolgsysteem. Personeelsvolgsystemen komen daarom vrij veel in organisaties voor.

Denk bijvoorbeeld aan een systeem waarin klantcontacten bij worden gehouden. Of systemen waarin dossiers worden bewaard en waarin wordt geregistreerd welke werknemer op welk moment een dossier raadpleegt.

Werkgever X moet het voorstel om een gps-tracker te installeren om locatiegegevens van de wagens waarin werknemers rijden te verzamelen en gebruiken ter instemming voorleggen aan de OR.

Het observeren en registreren van mensen en hun gedragingen is een hype in deze tijd van digitalisering. Ook binnen bedrijven en organisaties neemt het vastleggen van menselijke activiteiten hand over hand toe. Verzamelde gegevens kunnen opeens opduiken in beoordelingsgesprekken of aangelegde dossiers. Het is van belang dat hierover goed wordt gecommuniceerd tussen de werkgever en de werknemer. Goed werkgeverschap veronderstelt immers dat zorgvuldig wordt omgegaan met de persoonsgegevens van werknemers. De OR kan hieraan bijdragen: alle reden om het instemmingsrecht van de OR zorgvuldig toe te passen.

Als OR kunt u eventueel een beroep doen op het initiatiefrecht van artikel 23, derde lid, van de WOR wanneer u vindt dat de werkgever niet de noodzakelijke actie onderneemt.

Stemt u als OR niet in met het voorgenomen besluit van de werkgever? Dan kan de werkgever de kantonrechter om toestemming vragen op grond van artikel 27, vierde lid, WOR.

Twijfelt u als OR of er sprake is van een regeling voor het verwerken van persoonsgegevens van werknemers? Vraag dan de interne privacyfunctionaris om advies.

3. De Algemene verordening gegevensbescherming

Het wettelijk kader voor het verwerken van persoonsgegevens is vastgelegd in de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). De AVG stelt strikte eisen aan het verwerken van persoonsgegevens. Deze eisen zijn uitgewerkt in een aantal basisvoorwaarden. Bent u als OR al op de hoogte van deze belangrijke privacyregels?

Doelbinding
Volgens de AVG mogen persoonsgegevens alleen voor 'welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden' worden verzameld. De gegevens mogen vervolgens niet verder worden verwerkt op een manier die onverenigbaar is met die doeleinden. Dat noemen we 'doelbinding'. Eenvoudig gezegd: je mag gegevens die je voor het ene doel verzamelt, niet zomaar voor een ander doel gebruiken. Zeker niet als dit een totaal ander doel is.

Voorzieningen die persoonsgegevens registreren, kunnen al snel voor meerdere doeleinden worden ingezet. Denk bijvoorbeeld aan cameratoezicht. Dat kan niet alleen wordt gebruikt om werknemers en hun eigendommen te beveiligen, maar ook om werknemers tijdens het werk te observeren.

De werkgever (verwerkingsverantwoordelijke) moet het doel van de verwerking bepalen voordat hij begint met het verwerken van persoonsgegevens. Hierbij is van belang dat hij het doel van de verwerking zo nauwkeurig en volledig mogelijk omschrijft. Zijn er meerdere doelstellingen? Dan moet de werkgever deze afzonderlijk noemen en toetsen op de noodzaak om hiervoor persoonsgegevens te verzamelen.

In het voorstel voor het gps-trackerbeleid dat werkgever X aan de OR voorlegt, licht hij toe dat de locatiegegevens worden verzameld voor twee verschillende doelen:

- optimaliseren van de planning door werknemers naar de dichtstbijzijnde klanten te sturen;
- onderscheid maken tussen werk- en privékilometers in de kilometerregistratie.

Besluit werkgever X op een later moment dat hij de locatiegegevens ook voor een ander doel zou willen gebruiken? Dan is er sprake van een wijziging van de bestaande regeling. Werkgever X moet de nieuwe doelstelling toetsen aan de privacyregels en de wijziging voorleggen aan de OR.

Rechtmatigheid en behoorlijkheid
Persoonsgegevens moeten volgens de AVG worden verwerkt op een manier die rechtmatig, behoorlijk en transparant is voor de betrokkenen.

Persoonsgegevens mogen alleen worden verwerkt met een goede reden. De juridische naam hiervoor is 'rechtmatig'. In de AVG staan zes redenen (grondslagen) genoemd op basis waarvan persoonsgegevens rechtmatig mogen worden verwerkt. Bijvoorbeeld: de verwerking van persoonsgegevens is noodzakelijk om een overeenkomst uit te voeren, aan een wettelijke plicht te voldoen of een gerechtvaardigd belang te behartigen.

Een werkgever kan bijvoorbeeld een gerechtvaardigd belang hebben om persoonsgegevens van werknemers te verwerken om de bedrijfsveiligheid te verhogen. De werkgever moet hierbij wél altijd de privacybelangen van de werknemers uitdrukkelijk afwegen tegen zijn eigen belangen als werkgever. Die afweging moeten deugen, opgeschreven worden en transparant gecommuniceerd worden met werknemers.

Werkgever X licht in het voorstel toe dat de onderneming een goede reden heeft om een gps-tracker in te zetten. Maar alleen het noemen van deze goede reden is niet voldoende.

Werkgever X moet ook bepalen of het inzetten van de gps-tracker wel noodzakelijk is om zijn doelen te bereiken. Heeft Werkgever X nagedacht of het ook mogelijk is om een efficiënte route in te plannen zonder hiervoor locatiegegevens te gebruiken? En is er geen andere manier om onderscheid te maken tussen werk- en privékilometers, dus zonder gps-tracker? En weegt de goede reden van de werkgever wel op tegen de privacyschending van de werknemers?

Toestemming
Een van de mogelijke grondslagen is toestemming van degene om wie het gaat. Maar voor de meeste gegevensverwerkingen op het werk kan en mag de grondslag toestemming van de werknemer niet worden gebruikt. Omdat werknemers afhankelijk zijn van hun werkgever, kunnen zij meestal niet in vrijheid toestemming geven. Dus zonder zich onder druk gezet te voelen en zonder bang te zijn voor negatieve gevolgen. En toestemming die niet in vrijheid is gegeven, is volgens de AVG niet geldig. Alleen in zeer uitzonderlijke situaties kunnen werknemers vrije toestemming geven voor het verwerken van hun persoonsgegevens door de werkgever.

Bijzondere persoonsgegevens
Het is in principe verboden om bijzondere persoonsgegevens te verwerken. Tenzij er een wettelijke uitzondering geldt én de verwerkingsverantwoordelijke een grondslag heeft.

Voor meer informatie over grondslagen, zie dossier Mag u persoonsgegevens verwerken? op de website van de AP.

Juist en nauwkeurig
Persoonsgegevens moeten zoveel mogelijk juist zijn en zo nodig worden geactualiseerd. De werkgever moet maatregelen treffen om te waarborgen dat de gegevens juist en nauwkeurig zijn.

De werknemers van werkgever X rijden elk in een eigen wagen uit het wagenpark. Maar het komt soms voor dat er een wagen wegvalt, omdat deze bijvoorbeeld voor onderhoud bij de dealer staat. De werknemers lenen dan een andere wagen. Werkgever X moet ervoor zorgen dat de locatiegegevens niet zomaar aan de verkeerde werknemer worden gekoppeld. Gegevens die niet juist zijn moet Werkgever X wissen of corrigeren.

Informatieplicht
Werknemers moeten kunnen overzien wie hun gegevens verwerkt en voor welk doel. De werkgever heeft daarom een informatieplicht. Dat houdt in dat de werkgever werknemers moet laten weten wat er met hun gegevens gebeurt voordat de werkgever die gegevens daadwerkelijk verwerkt.

Bijvoorbeeld wanneer een nieuwe werknemer in dienst komt. De personeelsfunctionaris moet dan informatie verstrekken vóór het moment dat de werknemer de nodige formulieren invult voor de personeels- en salarisadministratie.

Dit geldt bijvoorbeeld ook als een werknemer een leaseauto krijgt. Van te voren moet de werknemer dan informatie krijgen over de gegevensverwerking bij autogebruik: welke gegevens worden vastgelegd en met welk doel.

Krijgt de werkgever gegevens niet van de werknemers zelf maar van een andere partij? Dan moet de werkgever de werknemers hierover informeren op het moment dat de werkgever de gegevens vastlegt.

Werkgever X moet de werknemers duidelijk informeren over zijn plan om gps-trackers te gebruiken. En over wat dit voor de werknemers betekent. Hoe werkt de gps-tracker? Waarom worden de locatiegegevens verzameld?

Dataminimalisatie
Persoonsgegevens moeten toereikend zijn, ter zake doen en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Eenvoudig gezegd: je mag niet meer gegevens verwerken dan je echt nodig hebt. Dat noemen we dataminimalisatie, oftewel zo min mogelijk gegevens verwerken.

Om te beoordelen of dit zo is, kunt u als OR de volgende vragen stellen:

- Maakt de werkgever voldoende gebruik van de mogelijkheden om persoonsgegevens te anonimiseren?
- Moet de werkgever de gegevens op individueel niveau verzamelen of kan de werkgever volstaan met gegevens op het niveau van een afdeling of van het bedrijf als geheel (geaggregeerd niveau)?
- Moet de werkgever over alle werknemers gegevens vastleggen? Of is het genoeg om informatie te verzamelen over werknemers in bepaalde functies of op bepaalde plaatsen?
- Kan de werkgever volstaan met een steekproef of moet de werkgever voortdurend gegevens vastleggen?

Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is om de doeleinden te bereiken waarvoor zij zijn verzameld. Dus: gegevens niet meer nodig? Verwijder ze!

Werkgever X heeft in het voorstel om gps-trackers te gebruiken toegelicht dat een van de doelen van het verzamelen van locatiegegevens is om werknemers naar de dichtstbijzijnde nieuwe klant te kunnen sturen. Om dit doel te bereiken, heeft werkgever X inzicht nodig in de huidige locatie van werknemers. Zodra de locatiegegevens niet meer actueel zijn, worden ze niet meer gebruikt voor dit doel. Voor het andere doel, de kilometerregistratie bijhouden, zijn de locatiegegevens zelf niet relevant: deze worden omgezet in de gereden afstand in kilometers.

De OR bevraagt werkgever X daarom kritisch over wat er met de (oude) locatiegegevens gebeurt. Worden deze direct gewist?

Beveiliging
Persoonsgegevens moeten op zo'n manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is. Dat moet gebeuren door passende technische of organisatorische maatregelen te nemen. Hierdoor moeten de gegevens onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging.

Om het noodzakelijke niveau van beveiliging te bepalen, moet de werkgever een risicoanalyse uitvoeren. Hierbij zijn onder meer de aard van de gegevens en de kring van gebruikers van belang.

Wilt u als OR beoordelen of de werkgever zicht heeft op de risico's die een (voorgenomen) regeling voor het verwerken van persoonsgegevens van werknemers met zich meebrengt? Dan kunt u de volgende vragen stellen:

- Wat doet de werkgever om de risico's tijdig in beeld te krijgen?
- Worden de risico's periodiek opnieuw beoordeeld?
- Is er een procedure vastgesteld om te testen of de beveiligingsmaatregelen (nog steeds) effectief zijn?

Zie verder *DPIA en voorafgaande raadpleging* (p. 12).

De werkgever moet ervoor zorgen dat de toegang tot de persoonsgegevens van betrokkenen wordt beperkt. Dat betekent bijvoorbeeld dat uitsluitend bevoegde werknemers toegang mogen hebben tot personeelsdossiers. Het is van belang dat de werkgever over beveiliging nadenkt voordat hij start met het verzamelen van persoonsgegevens. Beveiliging van persoonsgegevens moet binnen organisaties een blijvend punt van aandacht zijn.

Werkgever X licht in het gps-trackervoorstel toe dat alle werknemers een inlogcode krijgen waarmee ze toegang hebben tot de omgeving waarin de live locatie van de wagens beschikbaar is.

De werknemers van werkgever X vinden het geen fijn gevoel dat zij continu door al hun collega's in de gaten kunnen worden gehouden. Als de OR werkgever X hierop aanspreekt, blijkt dat hij hierbij nog niet had stilgestaan.

Bij het beantwoorden van de vraag wat een passende maatregel is, moet de werkgever rekening houden met de stand van de techniek.

Enkele voorbeelden van beveiligingsmaatregelen zijn:

- toegangsbeveiliging met meerfactorauthenticatie (identiteit van gebruiker controleren met minimaal twee verschillende typen authenticatiefactoren);
- registreren wie er toegang heeft gehad tot de gegevens (logging)
- pseudonimiseren van persoonsgegevens..

Als OR kunt u hierover advies inwinnen bij de information security officer of functionaris gegevensbescherming (FG) van uw organisatie. Ook vindt u hierover meer informatie op de website van de AP.

Ook wanneer er passende beveiligingsmaatregelen zijn genomen, kan er een datalek ontstaan. Dat houdt in dat er toegang is geweest tot persoonsgegevens of dat de gegevens zijn vernietigd, gewijzigd of vrijgekomen zonder dat dit de bedoeling was van de werkgever of zonder dat dit wettelijk was toegestaan. De werkgever is verplicht om een datalekregister bij te houden. Is er sprake van een ernstig datalek? Dan moet de werkgever dit datalek melden bij de AP en in sommige gevallen ook aan de betrokken.

Voor meer informatie, zie het onderwerp Beveiliging op de website van de AP.

Rechten van betrokkenen
Werknemers hebben verschillende privacyrechten. Hiermee kunnen zij controle houden over hun persoonsgegevens. Zo hebben zij onder meer recht op inzage in hun personeelsdossier. Ook kunnen zij vragen om rectificatie, aanvulling of verwijdering van hun gegevens. Hierdoor kunnen zij zich tegen onjuiste of incomplete gegevens in het dossier verweren.

Het personeel van werkgever X vindt het belangrijk om regelmatig de kilometerregistratie te kunnen controleren die wordt bijgehouden met de gps-tracker. Wijkt deze registratie niet af van de kilometerteller in de wagen? De OR vraagt werkgever X daarom hoe werknemers deze gegevens kunnen inzien.

Verwerkt de werkgever gegevens op grond van een gerechtvaardigd belang? Dan moet de werkgever de werknemers wijzen op het recht van bezwaar. Werknemers hebben het recht zich te verzetten tegen deze verwerking wanneer zij menen dat hun privacybelang zwaarder weegt dan het belang van de werkgever. Bijvoorbeeld wanneer er sprake is van bijzondere persoonlijke omstandigheden. De werkgever mag de gegevens vervolgens niet verwerken als de gerechtvaardigde gronden die de werkgever voor de verwerking aanvoert niet zwaarder wegen dan de belangen van de werknemers. Of als niet duidelijk is of deze gronden zwaarder wegen.

Ten slotte moet de werkgever werknemers de mogelijkheid bieden hun gegevens over te laten dragen. Dit heet het recht op dataportabiliteit. Werknemers kunnen hun persoonsgegevens dan in een gestructureerd, gangbaar en machineleesbaar formaat ontvangen. En deze gegevens vervolgens aan een andere organisatie overdragen.

Voor meer informatie, zie Rechten van betrokkenen op de website van de AP.

DPIA en voorafgaande raadpleging
Onder de AVG kan een verwerkingsverantwoordelijke verplicht zijn een data protection impact assessment (DPIA) uit te voeren voordat hij kan beginnen met het verwerken van gegevens. Een DPIA is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. Zodat er maatregelen kunnen worden genomen om deze risico's te verkleinen. Een DPIA is verplicht wanneer een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen.

De AP heeft een (niet-uitputtende) lijst opgesteld met soorten verwerkingen waarvoor een DPIA verplicht is. Het grootschalig of systematisch verwerken van persoonsgegevens om activiteiten van werknemers te monitoren staat op deze lijst. Dit valt dus onder de DPIA-plicht. Staat een verwerking niet op de lijst? Dan moet de werkgever zelf bepalen of de gegevensverwerking een hoog privacyrisico oplevert. Hiervoor kan de werkgever de 9 criteria gebruiken die de EU-privacytoezichthouders hebben opgesteld.

Werkgever X licht in het gps-trackervoorstel toe dat hij een DPIA heeft uitgevoerd en dat hij passende maatregelen zal nemen om alle risico's te beperken die in kaart zijn gebracht.

De OR wil graag meer weten over deze risico's en vraagt daarom of werkgever X de DPIA met de OR wil delen.

Blijkt uit de DPIA dat de gegevensverwerking een hoog risico oplevert? En kan de werkgever geen maatregelen vinden om dit risico te beperken? Dan moet de werkgever met de AP overleggen voordat hij met de verwerking mag starten. Dit wordt een voorafgaande raadpleging genoemd. De AP geeft dan advies

over hoe de werkgever de risico's van de voorgenomen verwerking kan beperken. De AP kan de werkgever ook adviseren om helemaal van de verwerking af te zien.

Is het niet verplicht om een DPIA uit voeren? Dan raadt de AP aan om een privacyrisicobeoordeling uit te voeren, als een vorm van goede bedrijfsvoering.

Verantwoordingsplicht
De verwerkingsverantwoordelijke moet kunnen aantonen dat hij aan de AVG-verplichtingen voldoet. Dat heet de verantwoordingsplicht. De AVG noemt een aantal verplichte maatregelen die de verwerkingsverantwoordelijke moet nemen om aan deze verantwoordingsplicht te voldoen.

Enkele voorbeelden zijn:

- een verwerkingsregister bijhouden;
- een risicobeoordeling (DPIA) uitvoeren (indien nodig);
- een datalekregister bijhouden.

Naast deze verplichte maatregelen zijn er andere maatregelen die de verwerkingsverantwoordelijke kunnen helpen om aan te tonen dat hij voldoet aan de eisen van de AVG. Bijvoorbeeld verantwoording afleggen in het jaarverslag of aansluiten bij een goedgekeurde gedragscode.

Functionaris gegevensbescherming
De functionaris gegevensbescherming (FG) is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. De FG geeft de verwerkingsverantwoordelijke advies en inzicht. Er zijn op grond van de AVG drie situaties waarin een organisatie verplicht is om een FG aan te stellen:

1. de organisatie maakt onderdeel uit van de overheid of is een publieke organisatie;
2. de kernactiviteit van de organisatie is om op grote schaal individuen te volgen of hun activiteiten in kaart te brengen;
3. de organisatie verwerkt op grote schaal bijzondere persoonsgegevens.

Is het niet verplicht om een FG aan te stellen? Dan kan de verwerkingsverantwoordelijke ervoor kiezen vrijwillig een FG aan te stellen.

De werkgever moet de FG naar behoren en op tijd betrekken bij alle zaken die te maken hebben met de bescherming van persoonsgegevens. Heeft u als OR al eens gesproken met de FG over de verwerking van persoonsgegevens van werknemers?

De OR heeft kennisgenomen van de DPIA voor de inzet van de gps-tracker. De risicobeoordeling van werkgever X roept wat nieuwe vragen op en de OR is benieuwd wat de FG daarvan vindt. De FG heeft een advies uitgebracht naar aanleiding van de DPIA. De OR vraagt het advies van de FG op en nodigt de FG uit om een toelichting te geven tijdens de volgende OR-bijeenkomst.

Gegevensverkeer met landen buiten de EU
Persoonsgegevens doorgeven naar een land buiten de Europese Unie (EU) is in principe alleen toegestaan als dat land een passend niveau van gegevensbescherming heeft. Dat betekent: gelijkwaardig aan het beschermingsniveau van de AVG. Is er geen sprake van een passend beschermingsniveau? Dan is doorgifte slechts toegestaan op grond van een van de wettelijke bepalingen uit de AVG.

Enkele voorbeelden van situaties waarin gegevens aan landen buiten de EU worden verstrekt:

- de werkgever heeft de salarisbetaling uitbesteed aan een salarisadministratiebureau (verwerker) buiten de EU;
- de werkgever maakt voor het opslaan van gegevens (waaronder ook persoonsgegevens) gebruik van de diensten van een cloudprovider, waarbij de gegevens op servers in de Verenigde Staten worden opgeslagen.

Het is van belang dat u als OR nagaat of de organisaties met wie de werkgever persoonsgegevens van werknemers deelt, gevestigd zijn in de EU.

Is de werkgever van plan een verwerker buiten de EU in te zetten om persoonsgegevens van werknemers te verwerken? Dan kunt u als OR de volgende vragen stellen:

- Is het nodig een verwerker buiten de EU in te zetten? Heeft de werkgever Europese verwerkers overwogen voor deze verwerking?
- Hoe wordt de bescherming van gegevens van werknemers gewaarborgd bij het verstrekken van hun persoonsgegevens aan de verwerker buiten de EU?

Werkgever X overweegt nog steeds om de locatiegegevens die worden verzameld door de gps-tracker te laten analyseren door een gespecialiseerd bedrijf. Omdat de locatiegegevens bij deze analyse voor een nieuw doel worden verwerkt, maakt werkgever X een nieuw voorstel en legt dat ter goedkeuring aan de OR voor.

De OR leest in de stukken dat de verwerker die werkgever X kiest om de locatiegegevens te analyseren de gegevens opslaat in een database buiten de EU. De OR vraagt werkgever X waarom hij voor deze verwerker kiest.

Voor meer informatie, zie Doorgifte binnen en buiten de EU op de website van de AP.

4. Toetsingsvragen voor personeelsvolgsystemen

Steeds meer werkgevers willen werknemers monitoren via personeelsvolgsystemen. Bijvoorbeeld als werknemers thuiswerken. Dit levert vragen op over de privacy van de werknemers. Welke vragen kunt u als OR hierover stellen?

Beoordeelt u personeelsvolgsystemen, dan kunt u krachtens artikel 27, eerste lid onder l. van de WOR de voorgestelde regeling op onderstaande punten toetsen. Heeft de organisatie een functionaris gegevensbescherming (FG)? Dan kan die u met advies terzijde staan.

1. Is er sprake van een personeelsvolgsysteem?
U heeft als OR instemmingsrecht als 'een voorziening is gericht op – of geschikt is voor – waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen' (artikel 27, eerste lid onder l. van de WOR). In het dagelijkse taalgebruik noemen we dergelijke 'voorzieningen' personeelsvolgsystemen. Is er sprake van een personeelsvolgsysteem, dan mag u ervan uitgaan dat er ook sprake is van verwerking van persoonsgegevens.

Vaak blijkt uit de opzet van een systeem dat het gericht is op het volgen van personeel. De wet voegt als criterium toe dat de instemming van de OR ook vereist is als een systeem daarvoor geschikt is. Er moet dus naar de mogelijke effecten van zo'n systeem worden gekeken. Kan het personeel worden gevolgd, ook al gebeurt dat in de praktijk (nog) niet? Dan is het toch een personeelsvolgsysteem.

Enkele voorbeelden van personeelsvolgsystemen zijn:

- een systeem dat aanwezigheid, tijd en toegang registreert;
- een track & trace-systeem in (vracht)auto's, zoals een gps-tracker, black box of boordcomputer;
- software die bijvoorbeeld toetsaanslagen, e-mailverkeer en/of internetgebruik van werknemers registreert;
- cameratoezicht op de werkplek;
- wearables, zoals een smartwatch;
- een systeem waarin klantcontacten worden bijgehouden;
- een systeem dat ondersteunt bij het afhandelen van werkzaamheden (workflow- of zaaksysteem);
- een voorziening binnen een systeem die inzage in (gevoelige) dossiers door werknemers registreert (logging);
- een systeem dat een pas of badge gebruikt om de aanwezigheid en/of plaats binnen een gebouw van een werknemer te registreren.

2. Is het nodig een personeelsvolgsysteem te gebruiken?
De volgende vraag die u als OR moet stellen, is of het gebruik van een personeelsvolgsysteem wel nodig is in de onderneming. Pas als het antwoord ja is, komt de manier waarop aan de orde.

Over de noodzaak van personeelsvolgsysteem kunt u als OR onder meer de volgende vragen stellen:

- Waarom is de werkgever van plan om deze voorziening te gebruiken? Of waarom wordt de voorziening gebruikt?
- Is er sprake van een wettelijke of contractuele verplichting? Zo niet, is het om een andere reden noodzakelijk om de voorziening in te voeren of te gebruiken?
- Is er geen van buiten komende noodzaak, kan de werkgever dan aantonen dat hij een legitieme reden (gerechtvaardigd belang) heeft om de voorziening te gebruiken?
- Hoe verhoudt het belang van de werkgever zich tot de belangen van de werknemers?
    - Hoe indringend is de observatie?
    - Komen de belangen van de werknemers in het gedrang?
    - Is het mogelijk om het doel dat de werkgever voor ogen heeft te bereiken op een voor de werknemers minder ingrijpende wijze?

Een personeelsvolgsysteem gebruiken is altijd een inbreuk op de privacy van werknemers. Hier moet niet te lichtvaardig over worden gedacht. Van belang is of de voorziening redelijk is in verhouding tot het beoogde doel. En of de werkgever ook met minder ingrijpende middelen kan volstaan.

De voorziening kan zo indringend zijn dat u als OR – vanuit de belangen van de werknemers en gelet op het doel – niet met de regeling wil instemmen. Of alleen onder voorwaarden. Dergelijke voorwaarden voor het gebruik van de voorziening kunnen in de regeling worden opgenomen.

Is de werkgever van plan om grootschalig en/of systematisch persoonsgegevens te verwerken om activiteiten van werknemers te monitoren? Dan moet de werkgever eerst een DPIA uitvoeren.

3. Worden de werknemers van tevoren op de hoogte gesteld van de observatie?
De werknemers moeten vooral informatie krijgen over:

- het doel van de observatie;
- het tijdschema en gebruik van de verzamelde gegevens;
- bewaartermijnen.

De werknemers moeten in elk geval hiervan op de hoogte worden gesteld op het moment dat het systeem wordt ingevoerd. Dit kan bijvoorbeeld met gedragsregels of een protocol.

Vragen die hierbij onder andere van belang zijn:

- Op welke wijze worden de persoonsgegevens ingezet?
- Wat zijn de eventuele gevolgen hiervan voor werknemers?
- Wie heeft er toegang tot de persoonsgegevens die worden verwerkt?
- Op welke manier wordt ongeoorloofde toegang gecontroleerd?

Structurele heimelijke observatie is niet toegestaan. Incidenteel kan heimelijke controle gerechtvaardigd zijn, mits aan strenge (extra) voorwaarden is voldaan. Er moet sprake zijn van een redelijke verdenking over een of meer werknemers die de inzet van zo'n zware controle rechtvaardigt. Hierbij is vereist dat andere middelen zijn uitgeput. En dat er een zwaarwegend belang van de onderneming in het geding is. Werknemers moeten weten dat in uitzonderlijke situaties heimelijk een personeelsvolgsysteem kan worden ingezet. Voor het heimelijk controleren van werknemers geldt een DPIA-verplichting.

Vragen die u als OR kunt stellen over heimelijke monitoring:

- Is in de organisatie bekend welk gedrag niet wordt getolereerd en zijn werknemers hiervoor gewaarschuwd?
- Heeft de werkgever op een andere manier geprobeerd om het schadelijke gedrag te voorkomen of te achterhalen?
- Is voldoende gewaarborgd dat de voorziening niet lichtvaardig wordt ingezet?

4. Wordt de personeelsbeoordeling uitsluitend gebaseerd op de gegevens die met persoonsvolgsystemen zijn verzameld?
Van belang is dat gegevens niet zomaar worden vastgelegd in de personeelsadministratie. En dat niet uitsluitend op grond hiervan personeelsbeoordeling plaatsvindt. Verder moeten werknemers kort na de observatie door het personeelsvolgsysteem de kans krijgen om te reageren op de resultaten. Hun visie hierop moet bij de resultaten worden gevoegd.

Meer weten? Bekijk ook de informatie op de website van de AP en/of de website van uw sector- of brancheverenigingen.