ICTRECHT

FACTSHEET PRIVACY EN MONITORING OP DE WERKVLOER

Op 25 mei 2018 treedt de AVG in werking. Dit betekent dat strenger en meer zal worden gehandhaafd op privacy (boetes kunnen oplopen tot wel 20 miljoen euro). Voor bedrijven is het dus van groot belang om 'AVG-Proof' te worden. Waar moet je als bedrijf dan rekening mee houden ten aanzien van de privacy van werknemers? De Article 29 Working Party (WP29) heeft een opinie opgesteld waarin de privacywet wordt uitgelegd in het licht van gegevensverwerking op het werk. In deze factsheet vatten we de regels kort samen. Aan het eind vind je een aantal handige voorbeelden.

1 | WAT IS EEN WERKNEMER?

Van een arbeidsrelatie is sprake als een natuurlijke persoon arbeid verricht tegen loon, onder het gezag van een ander. Degene die de arbeid verricht onder het gezag van de ander en hiervoor loon ontvangt, wordt aangemerkt als de werknemer. Hierbij is niet noodzakelijk dat er daadwerkelijk een arbeidscontract is getekend, er wordt gekeken naar alle omstandigheden van het geval. Iemand die bijvoorbeeld volgens zijn contract bij een bedrijf stage loopt, kan in de praktijk soms ook als werknemer worden aangemerkt als de werkzaamheden meer zijn gericht op het behalen van economisch voordeel dan op het eigen leren en ontwikkelen in het vakgebied.

WP29 spreekt in het opiniestuk over 'werknemer', maar bedoelt daarmee ook de natuurlijke personen die daarmee te vergelijken zijn, zoals freelancers en stagiairs. Natuurlijke personen die een vergelijkbare positie als een werknemer hebben, genieten dezelfde bescherming.

2 | WAT VOOR PERSOONSGEGEVENS VERWERKT EEN WERKGEVER?

Een werkgever verwerkt persoonsgegevens van al zijn werknemers. Hij verwerkt bijvoorbeeld NAW-gegevens, bankrekeningnummers, contactgegevens en salarisgegevens. Dat werkgevers deze informatie verwerken is vanzelfsprekend en vaak verplicht, maar daarnaast kunnen werkgevers ook nog allerlei andere persoonsgegevens van werknemers verwerken.

Mede door de sterke digitalisering, nemen de technische middelen en mogelijkheden om werknemers in de gaten te houden aanzienlijk toe. Denk aan:

- Camerabeelden van videobewaking;
- Informatie van software die het gebruik van internet- en e-mailverkeer bijhoudt en analyseert;
- Opnames van telefoongesprekken of chatberichten;
- Op afstand beheren van alle mobiele apparatuur, zoals telefoons en laptops;
- Tracking- of locatiegegevens van bedrijfsauto's of apparatuur. Hiervoor kan een nieuwe rechtspersoon worden opgericht maar er kan ook gebruikgemaakt worden van reeds bestaande entiteiten zoals de holding.

3 | WAAROM IS EXTRA AANDACHT VOOR PRIVACY OP DE WERKVLOER BELANGRIJK?

Dat er technisch gezien veel meer mogelijkheden zijn om werknemers in de gaten te houden, wil nog niet zeggen dat dit juridisch ook is toegestaan. Voor een rechtmatige verwerking van persoonsgegevens is in elk geval een wettelijke grond nodig. De wettelijke gronden zijn:

- Noodzakelijk voor de uitvoering van de arbeidsovereenkomst;
- Noodzakelijk om te voldoen aan een wettelijke plicht;
- Noodzakelijk om vitale belangen van werknemer/een ander natuurlijk persoon te beschermen;
- Noodzakelijk voor de vervulling van een taak van algemeen belang of in uitoefening van openbaar gezag;
- Noodzakelijk voor behartiging van gerechtvaardigde belangen van de werkgever of een derde, tenzij fundamentele belangen van werknemer zwaarder wegen.
- Toestemming van werknemer voor een of meer specifieke doeleinden.

ICTRecht Noord-Nederland Helperpark 288E 9723 ZA Groningen
ictrecht.nl | info@ictrecht.nl | 050 209 3499

ICTRecht Amsterdam Jollemanhof 12 1019 GW Amsterdam
ictrecht.nl | info@ictrecht.nl | 020 663 1941

Terwijl toestemming in het algemeen een van de belangrijkste en meest gebruikte wettelijke grondslagen is voor verwerking van persoonsgegevens, is dat op de werkvloer juist niet zo. Doordat de werkgever gezag heeft over de werknemer, kan toestemming van een werknemer aan een werkgever in principe niet vrijwillig gegeven worden. Doordat de werkgever gezag uitoefent over de werknemer en de werknemer bovendien financieel afhankelijk is van de werkgever, zal een werknemer zich vrijwel nooit vrij genoeg voelen om toestemming te weigeren of in te trekken.

Doordat werkgevers de verwerking van persoons-gegevens van werknemers niet op de grond toestemming kunnen baseren, moet een andere wettelijke grondslag van toepassing zijn. Als werkgever is het ook van belang om niet te gemakkelijk aan te nemen dat het eigen belang, of dat van een derde, de verwerking kan rechtvaardigen. Voor het toepassen van deze grondslag is namelijk een zorgvuldige belangenafweging nodig, waarbij de noodzaak en proportionaliteit van de verwerking moet kunnen worden aangetoond. Wanneer een werkgever dit niet kan aantonen voor alle persoonsgegevens die worden verwerkt, bijvoorbeeld als er ook een oplossing mogelijk is met minder impact op de privacy van de werknemer, kunnen boetes en aansprakelijkheid het gevolg zijn.

4 | WAT IS EEN PROPORTIONALITEITS-TOETS OF PIA?

De belangenafweging die de werkgever moet maken om te bepalen of er voldoende rechtsgrond bestaat voor de verwerking, wordt de proportionaliteitstoets genoemd. Deze toets kan een werkgever zelf (laten) doen door voor elke verwerking van persoonsgegevens van werknemers een PIA (privacy impact assessment) te doorlopen. Een PIA moet in ieder geval worden doorlopen als nieuwe technologie wordt gebruikt die een grote hoeveelheid data genereert of verwerkt.

De PIA is een hulpmiddel voor het uitvoeren van de proportionaliteitstoets, waarin rekening wordt gehouden met alle omstandigheden van het geval. De werkgever maakt dan een afweging tussen zijn eigen legitieme belangen en de redelijke verwachting van privacy van werknemers. De specifieke technologie die wordt gebruikt moet noodzakelijk zijn, in verhouding staan tot het na te streven doel en geïmplementeerd zijn op een manier die de privacy van werknemers zo min mogelijk beperkt.

Het zo privacyvriendelijk mogelijk inrichten van systemen wordt ook wel ‘privacy by design’ genoemd. Daarnaast moet je aan werknemers kunnen aantonen dat maatregelen zijn genomen om de juiste balans te treffen tussen het gerechtvaardigd belang van de werkgever en het fundamentele recht van de werknemer (de privacy).

Legitieme belangen zouden kunnen zijn:

- Detecteren en voorkomen van verlies van intellectueel of materieel bedrijfseigendom;
- Verbeteren van productiviteit van werknemers;
- Verbeteren van de bescherming van persoonsgegevens die het bedrijf verwerkt.

5 | WELKE VERWERKINGEN MOGEN NIET OF BIJNA NOOIT?

Een aantal verwerkingen moet, ondanks een eventueel gerechtvaardigd belang, altijd worden vermeden. Hier weegt de privacy van de werknemer altijd zwaarder:

- Monitoring in gevoelige ruimten, zoals sanitaire-, religieuze- en pauzeruimten;
- Geautomatiseerde beslissingen over bijvoorbeeld prestaties;
- Continu monitoren in plaats van steekproefsgewijs;
- Heimelijke opnames mogen alleen in zeer uitzonderlijke gevallen, zoals bij een gegronde verdenking van een strafbaar feit of het lekken van bedrijfsgeheimen.

6 | WELKE PLICHTEN HEEFT EEN WERKGEVER OM PRIVACY IN DE WERKSFEER TE WAARBORGEN?

Bij verwerking moet werkgever de privacy zoveel mogelijk blijven waarborgen. De werkgever heeft daarom een aantal verplichtingen:

- Gegevens moeten adequaat, relevant en niet te vergaand voor het legitieme doel zijn;
- Is er binnen een organisatie een ondernemingsraad, dan moet deze toestemming geven voor het gebruik van personeelsvolgsystemen;
- Het gebruik, het doel en de manier van verwerking moeten duidelijk kenbaar worden gemaakt aan de werknemers (transparantie);
- Aan werknemers moet de mogelijkheid worden gegeven om hun rechten uit te oefenen (inzage, correctie, verwijdering en blokkering);
- Persoonsgegevens moeten worden verwijderd waar mogelijk, en niet langer bewaard dan nodig;
- Persoonsgegevens moeten worden beveiligd door passende technische en organisatorische maatregelen.

7 | WAT MOET EEN WERKGEVER DOEN OM PERSOONSGEGEVENS TE BEVEILIGEN?

Belangrijk om te weten is dat de wet geen specifieke maatregelen of beveiligingsstandaard voorschrijft. Volgens de wet moet de beveiliging passend zijn voor de gevoeligheid van de gegevens en de risico's die met de verwerking samenhangen. Ook de kosten van de maatregelen wegen daarbij mee.

Dat neemt niet weg dat het toepassen van een standaard (zoals ISO 27001, 27002, 27017, 27018, of NEN 7510, 7512, of 7513) een goed hulpmiddel kan zijn om tot de wettelijk vereiste 'passende' beveiliging te komen. Het is ook mogelijk dat bepaalde maatregelen of standaarden in een bepaalde sector zó gemeengoed worden, dat het erg lastig kan worden om aan te tonen dat de beveiliging toch passend is zonder deze maatregelen of standaarden toe te passen. Zo lijkt het bijvoorbeeld de vraag of er vandaag de dag nog serieuze hostingproviders zijn die helemaal geen ISO 270xx standaard hebben geïmplementeerd.

Enkele voorbeelden van gebruikelijke beveiligings-maatregelen:

- Beveiligings- en autorisatiebeleid (toegang alleen bij need-to-know);
- Logische toegangscontrole (sterke wachtwoorden en/of multi-factor-authenticatie);
- Patch management (voor tijdige uitrol beveiligingsupdates);
- Beveiliging van internetverbindingen (bijvoorbeeld via SSL/TLS-technologie);
- Beveiliging van interne netwerken (firewalls, met de juiste configuratie);
- Antivirussoftware;
- Encryptie (versleuteling) van apparaten of databases met persoonsgegevens;
- Fysieke toegangsbeveiliging (zoals hekken, sloten, alarmsystemen, camera's).

Uiteraard verdient het ook aanbeveling om periodiek te controleren of de maatregelen correct zijn geïmplementeerd en goed werken.

Wat in elk geval niet vergeten mag worden, is om met alle externe partijen die persoonsgegevens van werknemers kunnen verwerken, bijvoorbeeld een salarisadministrateur, arbodienst, of pensioenverzekeraar of -tussenpersoon, goede afspraken over de verwerking en beveiliging van persoonsgegevens vast te leggen in de verplichte verwerkersovereenkomst (voor ingang van de AVG heet dit 'bewerkersovereenkomst'). Met onze generator maakt u eenvoudig een verwerkersovereenkomst.

8 | WAAR MOET DE WERKGEVER ACTIEF DUIDELIJKE INFORMATIE OVER GEVEN?

De informatieplicht is op de werkvloer van groot belang. De werkgever kan aan deze verplichting voldoen door middel van een interne privacyverklaring of een intern privacyreglement. Dit beleid moet op een duidelijke manier worden aangekondigd en gemakkelijk kunnen worden teruggevonden en bekeken. Je kunt het beleid bijvoorbeeld aan iedere nieuwe medewerker verstrekken en het daarnaast opnemen in het medewerkersportaal. Wanneer het beleid wordt vernieuwd, is het ook van belang dat medewerkers daarvan op de hoogte worden gesteld.

In het beleid moet in ieder geval worden opgenomen: Of en wanneer monitoring van werknemers wordt toegepast;

- De doeleinden van gegevensverwerking;
- De middelen die gebruikt worden voor gegevensverwerking;
- Een overzicht van de gegevens die worden bijgehouden met bijbehorende bewaartermijn;
- Wie wanneer toegang heeft tot welke gegevens;
- Hoe de gegevens beveiligd worden;
- Welke rechten de werknemer heeft.

De informatieplicht geldt daarnaast ook nog achteraf. De werknemers die zijn gemonitord of gecontroleerd, moeten hiervan achteraf nogmaals door werkgever op de hoogte worden gebracht.

Maak met onze generatoren eenvoudig een ICT- en internetreglement, cameratoezicht reglement of BYOD-reglement.

9 | WAT MAG EEN WERKGEVER MET GEGEVENS DIE DOOR MONITORING ZIJN VERKREGEN?

Zeer belangrijk is het doelbindingsvereiste. Een werkgever moet er op letten dat resultaten van monitoring van (handelingen van) werknemers alleen worden gebruikt voor het doel waarvoor ze zijn verkregen. Resultaten van monitoring die zijn toegepast ter voorkoming van datalekken of ter bestrijding van fraude, mag je dus niet gebruiken om medewerkers te beoordelen op functioneren. Het doel van geautomatiseerd monitoren mag nooit zijn het beoordelen van werknemers en het nemen van beslissingen ten aanzien van arbeidsvoorwaarden.

10 | EEN AANTAL PRAKTISCHE VOORBEELDEN

Hieronder vindt u een aantal voorbeelden om te helpen de privacyregels in de praktijk correct toe te passen, in overeenstemming met de opinies van WP29.

10.1 | SOCIAL MEDIA EN HET AANTREKKEN VAN NIEUW PERSONEEL

Een potentiële nieuwe werknemer controleren via internet, door bijvoorbeeld social media accounts te bezoeken, mag dat? De afweging kan hier gemaakt worden door het beantwoorden van een aantal vragen. Is het social media account gerelateerd aan professionele doelen? Is de informatie op het account relevant voor de baanprestatie? Voor het gebruik van de gegevens in een sollicitatieprocedure, moet je op deze vragen ja kunnen antwoorden. Komt uit je afweging dat je een voldoende gerechtvaardigd belang hebt, dat opweegt tegen het privacybelang van werknemer en er geen minder ingrijpende middelen mogelijk zijn? Dan mag je de social media accounts bezoeken, maar volgens de opinie van WP29 is het wel nodig dat kandidaten daarover worden geïnformeerd, bijvoorbeeld door daar in de vacature nadrukkelijk op te wijzen.

10.2 | SOCIAL MEDIA CONTROLEREN VAN OUD-PERSONEEL

Als werkgever kan het wenselijk zijn om het LinkedIn-profiel van een oud-werknemer in de gaten te houden. Om bijvoorbeeld te controleren of diegene het concurrentiebeding niet overtreedt. Dit is een gerechtvaardigd belang, dat tegen de privacy van de werknemer opweegt, als er geen andere minder ingrijpende manier mogelijk is. Ook hier geldt weer de informatieplicht vooraf.

10.3 | CAMERATOEZICHT IN KANTOORRUIMTEN

Voor elke camera die je als werkgever ophangt, moet je bepalen wat het gerechtvaardigde belang hiervoor is. Wil je bedrijfseigendommen beveiligen? Dat is een gerechtvaardigd belang, dat op zou kunnen wegen tegen de privacy van de werknemer. Minder ingrijpende middelen zijn echter ook vaak mogelijk. Hang bijvoorbeeld een bewegingssensor op of hang de camera zo op, dat deze niet op de werkplek van werknemers gericht is.

De camera mag er in ieder geval niet hangen om werknemers te controleren en om prestaties of aanwezigheid te beoordelen. Ook gezichtsherkenning is in principe niet toegestaan. Hierbij blijft het weer belangrijk dat werknemers vooraf goed worden geïnformeerd. Waar hangt de camera? Hoe lang worden beelden bewaard? Wie mogen en wie kunnen de beelden bekijken?

10.4 | CONTROLE VAN GEBRUIK VAN ICT-VOORZIENINGEN EN IN- EN UITGAANDE COMMUNICATIE

Het is wettelijk verplicht om persoonsgegevens te beveiligen tegen verlies en onrechtmatige verwerking. De manier waarop dit moet gebeuren is echter niet in de wet vastgelegd. Om datalekken via e-mail te voorkomen, zou bijvoorbeeld een datalek preventie systeem kunnen worden overwogen, waarbij uitgaande e-mails automatisch gescand worden. Deze moet dan wel zo worden ingeregeld dat de impact op privacy van eigen werknemers wordt beperkt tot het strikt noodzakelijke.

Bij dergelijke systemen kunnen namelijk aanzienlijke risico's bestaan op 'false positives', waardoor controles plaatsvinden waarbij persoonsgegevens worden verwerkt, terwijl dat achteraf onterecht blijkt. Voor de transparantie zou het daarbij ook wenselijk zijn om duidelijk te vermelden op basis van welke eigenschappen (zoals woorden, of bijlagen) een bericht kan worden geblokkeerd en/of nader gecontroleerd, zonder daarbij afbreuk te doen aan de effectiviteit van de maatregel. Het bijhouden van ál het gebruik van applicaties, alle toetsenbordaanslagen en muisbewegingen voor het controleren op handelingen in verband met data, wordt door privacytoezichthouders praktisch nooit als proportioneel gezien.

10.5 | TRACKING VAN HET VERVOERSMIDDEL WAARMEE DE WERKNEMER ZICH VOORTBEWEEGT

Voor veel vervoersmiddelen is het mogelijk om via GPS de locatie real-time te volgen en eventueel zelfs extra informatie over het voertuig op afstand te verkrijgen. Een werkgever kan belang hebben bij het volgen van de scooter van een pizzabezorger of de locatie te weten van een vrachtwagen. Een gerechtvaardigd belang kan zijn het voertuig terugvinden na diefstal. Het real-time in kunnen zien van locatiegegevens zal meestal te veel inbreuk maken op de privacy van de werknemer die zich ermee verplaatst. Minder ingrijpend zou zijn om de locatiegegevens pas beschikbaar te maken als het vervoersmiddel bijvoorbeeld als gestolen is opgegeven of als de ramen zijn ingebroken.

VRAGEN?

Neem contact op met Demi Grandiek of Matthijs van Bergen via 020 663 1941 of info@ictrecht.