WEES U BEWUST VAN DE PRIVACYRISICO'S BIJ HET NIEUWE WERKEN

Let ook op privacy buiten het kantoor!

Het Nieuwe Werken kan verschillende privacyrisico's met zich meebrengen. Nu de Algemene verordening gegevensbescherming (AVG) van toepassing is, is het nog belangrijker om hier alert op te zijn. Mag u uw werknemers bijvoorbeeld volgen via wifitracking? En hoe gaat u om met de privacy van werknemers die hun eigen smartphone of laptop gebruiken voor het werk?

Het Nieuwe Werken zorgt ervoor dat werknemers op een andere manier gaan werken. Hierbij komen ook andere privacyrisico's om de hoek kijken. Doordat werknemers vanaf een andere plek gaan werken, hebben werkgevers soms het gevoel dat zij de grip kwijtraken. Er ontstaan daardoor nieuwe behoeften om te controleren of werknemers wel echt aan het werk zijn, denk bijvoorbeeld aan wifitracking. Via wifitracking-technologie worden locatiegegevens van een mobiel apparaat – zoals een tablet of smartphone – opgeslagen en verwerkt. Mobiele apparaten kunnen op drie manieren getrackt worden: via gsm-signalen, bluetooth en wifi. Het apparaat hoeft niet per se verbonden te zijn met wifi om getrackt te worden. Via wifitracking-technologie kan een werkgever precies zien en bijhouden waar een werknemer zich bevindt. Het gebruik van deze technologie vormt dus een inbreuk op de persoonlijke levenssfeer van de werknemer. Toch mag een werkgever onder omstandigheden deze technologie toepassen.
Bij wifitracking verwerkt de werkgever locatiegegevens die herleidbaar zijn naar de werknemer. De verwerking van deze persoonsgegevens is toegestaan als het gebaseerd is op een wettelijke grondslag uit de AVG. Eén van deze grondslagen is toestemming van de betrokkene.
Als een werknemer dus specifieke, op informatie berustende, toestemming heeft verleend voor wifitracking, dan zou de werkgever dit in principe kunnen toepassen. Een werkgever kan hiervoor bijvoorbeeld een aparte app gebruiken of incheckmethoden bedenken voor bepaalde locaties. U kunt echter niet te makkelijk aannemen dat er sprake is van toestemming van de werknemer, omdat er tussen de werkgever en de werknemer sprake is van een afhankelijkheidsrelatie (zie kader linksonder).

Belang

Aangezien toestemming in de werkgever-werknemerrelatie vaak geen stand houdt, kunt u beter onderbouwen dat wifitracking noodzakelijk is voor het behartigen van een gerechtvaardigd belang. Vaak zal een werkgever wifitracking willen inzetten om een werknemer te controleren. In principe is dit niet toegestaan, tenzij er zich een bijzondere situatie voordoet. Het belang van uw organisatie moet zwaarder wegen dan het belang van de werknemer bij het behouden van zijn privacy.
Daarnaast mag de gekozen werkwijze niet verder gaan dan strikt noodzakelijk is om het doel te bereiken. Verder moet u aantonen dat het doel niet met minder ingrijpende middelen te realiseren is. Het afbakenen van de periodes en locaties is daarbij een vereiste. ▸▸▸

Zeer terughoudend omgaan met toestemming

Het geven van toestemming is weliswaar een wettelijke grondslag voor het verwerken van persoonsgegevens onder de AVG, maar in de arbeidsrelatie moet u hier zeer terughoudend mee omgaan. De reden hiervoor is dat de toestemming aan een groot aantal eisen moet voldoen. Eén van de vereisten is dat de betrokkene vrij moet zijn om zijn toestemming te weigeren en vrij moet zijn om zijn toestemming op ieder willekeurig moment in te trekken. Dit ligt vaak lastig in een arbeidsrelatie. Vanwege de afhankelijkheidsrelatie tussen werkgever en werknemer kunt u er dus niet blindelings op vertrouwen dat de gegeven toestemming van een werknemer in een eventuele rechtszaak overeind blijft. De belangenafweging heeft als grondslag dan ook duidelijk de voorkeur boven toestemming.

Het verrichten van metingen binnen afgesproken locaties – bijvoorbeeld bij een bezoek aan een bedrijf of op de thuiswerkplek – is namelijk minder ingrijpend dan wanneer de metingen ongelimiteerd plaatsvinden. Let erop dat u altijd zo veel als mogelijk is rekening houdt met de privacy van de werknemer. Een maatregel de hieraan bijdraagt is dat uw organisatie de gegevens binnen 24 uur na de vastlegging anonimiseert.

Stel een bewaartermijn in voor de gegevens

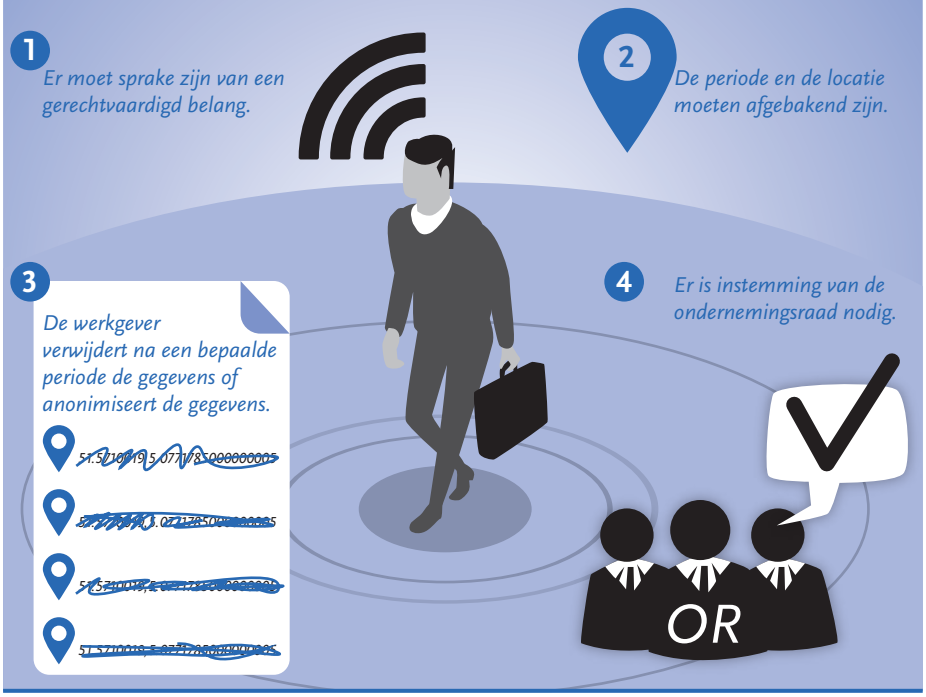
Het verwerken van gegevens door middel van wifitracking of vergelijkbare technieken houdt in dat uw organisatie locatiegegevens van een werknemer opslaat, samen met de unieke identifier van het apparaat. Omdat deze meetgegevens herleidbaar zijn naar individuele werknemers, mag u ze slechts een bepaalde periode bewaren. U moet hiervoor bewaartermijnen vaststellen en kunnen onderbouwen waarom de gekozen bewaartermijn noodzakelijk is voor het beoogde doel van de metingen. Na het verstrijken van de bewaartermijn moet uw organisatie de gegevens vernietigen of anonimiseren.

Bring your own device

Een ander privacyvraagstuk dat zich kan voordoen bij Het Nieuwe Werken is hoe u omgaat met werknemers die hun privé-smartphone, -laptop of -tablet gebruiken voor het werk, oftewel bring your own device. Dit betekent ook dat werknemers bepaalde documenten op deze apparaten kunnen opslaan die vertrouwelijke of bedrijfsgevoelige informatie bevatten. Het is verstandig om hiervoor beleid op te stellen. Hierin kunt u opnemen onder welke voorwaarden het is toegestaan om eigen apparaten te gebruiken en aan welke beveiligingseisen deze moeten voldoen. Zo kunt u bijvoorbeeld opnemen dat werknemers vertrouwelijke gegevens en bedrijfsgevoelige informatie altijd moeten beveiligen met een wachtwoord. Geef in dit beleid ook aan welke sancties uw organisatie neemt als werknemers de regels overtreden. Het is bovendien verstandig om het beleid deel te laten uitmaken van de arbeidsovereenkomst of naar het beleid te verwijzen in de arbeidsovereenkomst. U kunt dan bewijzen dat u de werknemer van de regels op de hoogte heeft gesteld, doordat zij hiervoor hebben getekend.

Voorwaarden voor wifitracking

Via wifitracking kunnen werkgevers via de apparatuur van werknemers bijhouden waar zij zich bevinden. Hiervoor gelden wel een aantal privacyvoorwaarden:



Monitoren

Naast de bescherming van uw bedrijfsgegevens moet u bij bring your own device ook extra letten op de privacy van uw werknemers. Als werknemers hun privéapparatuur gebruiken, gelden er namelijk strengere privacyregels voor het monitoren van het internetgedrag of telefoongebruik van werknemers. Als voorwaarde geldt dat de controles alleen worden uitgevoerd met een duidelijk doel dat van tevoren omschreven is. Denk aan het bewaken van bedrijfsgeheimen of het voorkomen van seksuele intimidatie. Daarnaast moeten de controlemaatregelen in verhouding staan tot de belangen van de werknemer.
Verder moet u aangeven op welke manier het toezicht plaatsvindt, wie dit toezicht voor zijn rekening neemt, wie toegang heeft tot de gegevens en hoe lang uw organisatie de gegevens bewaart. Ook deze zaken neemt u op in het beleid of de gedragscode van uw organisatie. Let erop dat de OR instemming heeft op het instellen, wijzigen of intrekken van een gedragscode waarin de controle op apparaten is geregeld (zoals wifitracking of monitoring). Dit geldt ook als de controle niet gericht is op het volgen van personeel, maar daarvoor wel geschikt is.

Hibby Giard, advocaat bij Ausma de Jong Advocaten te Utrecht, tel. 06 55 16 35 18, e-mail: giard@ausmadejong.nl, www.ausmadejong.nl