

Wat zijn de regels bij het monitoren van werknemers?



Werkgevers kunnen hun werknemers monitoren op de werkvloer of als ze thuiswerken. Dat is op zich niet verboden, zolang ze maar rekening houden met het recht op privacy van werknemers vanuit de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet AVG (UAVG). Ook vanwege goed werkgeverschap moeten ze de persoonlijke levenssfeer van hun werknemers respecteren.

Het monitoren van werknemers kan bijvoorbeeld met een track & trace-systeem in bedrijfswagens (zoals een gps-tracker), met volgsoftware die registreert wat de werknemer op zijn computer doet en monitoring-apps of wearables (bijvoorbeeld een smartwatch) die iemands gezondheid meten. Daarnaast kan sprake zijn van meer traditionele monitoring zoals het opnemen van telefoongesprekken, het nagaan van e-mails of toezicht met een camera op de werkvloer.

Voor een werkgever met een controle start, moet hij bepalen met welk doel hij controleert. Van dat doel hangt af hoe omvangrijk de controle mag zijn en hoe die mag plaatsvinden. Doelen kunnen bijvoorbeeld zijn: systeem- en netwerkbeveiliging, beschermen van bedrijfsgeheimen of minder kosten en tijdsverlies.

Als een organisatie een ondernemingsraad (OR) heeft, moet de werkgever vooraf instemming vragen aan de OR bij een regeling voor het gebruik van personeelsgegevens en als hij een personeelsvolgsysteem gaat gebruiken. De OR mag zich ook op eigen initiatief uitspreken over het gebruik van gegevens van werknemers door de werkgever.

Werknemers hebben recht op vertrouwelijke communicatie

Voorwaarden voor controle en monitoring van werknemers

Belangrijke voorwaarden voor de controle van werknemers zijn:

- Een gerechtvaardigd belang dat zwaarder weegt dan de rechten en belangen van de werknemers, waaronder hun recht op privacy. De werkgever moet dat kunnen onderbouwen.
- Er moet een noodzaak zijn voor het monitoren van de werknemers. Dat betekent dat de werkgever zijn doel niet op een andere, minder ingrijpende manier kan bereiken.
- De werkgever moet de werknemers informatie verstrekken over wat wel en niet mag, dat controle mogelijk is en hoe die plaatsvindt. De werkgever moet zijn werknemers vooraf informeren dat zij gecontroleerd kunnen worden. Hij kan de werknemers bijvoorbeeld informeren met gedragsregels in een personeelsreglement of een protocol.
- Werknemers hebben recht op vertrouwelijke communicatie via bijvoorbeeld e-mail of telefoon. Werkgevers mogen geen e-mails bekijken of gesprekken beluisteren die duidelijk privé zijn.

Stelselmatig monitoren van persoonsgegevens

Werkgevers die grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens willen inzetten om activiteiten van werknemers te controleren, moeten eerst een data protection impact assessment (DPIA) toepassen.

Voorbeelden waar dit nodig is, zijn controle van e-mail en internetgebruik, gps-trackers in (vracht)auto's van werknemers en cameratoezicht om diefstal en fraude te bestrijden. Als de organisatie een functionaris gegevensbescherming (FG) heeft, moet de werkgever deze om advies vragen bij het toepassen van de DPIA.

Uit een DPIA kan naar voren komen dat een gewenste controle voor een hoog risico zorgt. Als het de werkgever dan niet lukt om maatregelen te treffen om dat risico te beperken, moet hij met de Autoriteit Persoonsgegevens (AP) overleggen voordat hij met de controle van werknemers begint. Dit staat bekend als een voorafgaande raadpleging. Een FG kan adviseren of een voorafgaande raadpleging nodig is.

Een werkgever moet hij zich bij heimelijke controle houden aan een aantal extra eisen

Heimelijke controle van werknemers

Het heimelijk (stiekem) controleren van werknemers is normaal gesproken niet toegestaan. Als een werkgever dat toch doet, moet hij zich houden aan een aantal extra eisen voor heimelijke controle naast de normale eisen. Deze zijn:

- De werkgever heeft een redelijke verdenking dat één of meer werknemers iets doen wat strafbaar of verboden is.
- Lukt het een werkgever ondanks veel inspanningen niet om de diefstal of fraude te beëindigen, dan kan hij echt niet anders dan werknemers heimelijk controleren.
- De heimelijke controle is incidenteel. De werkgever mag de heimelijke controle alleen uitvoeren in een vooraf bepaalde periode. Hij mag werknemers dus niet voortdurend heimelijk controleren.
- De werkgever moet de betrokken werknemer(s) altijd achteraf informeren over de heimelijke controle. Dat geldt ook als uit de controle niet bleek dat een verdenking gegrond was.
- Controleert de werkgever voor het eerst heimelijk, dan moet hij vooraf een DPIA uitvoeren. Een DPIA is niet nodig voor iedere volgende keer dat de werkgever een incidentele heimelijke controle uitvoert met een werkwijze die gelijk is aan de eerste keer. Daarnaast hoeft de werkgever ook geen DPIA uit te voeren bij bestaand beleid voor heimelijke controle, dat de AP vanuit de voormalige Wet bescherming persoonsgegevens heeft goedgekeurd na voorafgaand onderzoek. De verwerking mag dan in de tussentijd niet zijn veranderd.

Opnemen van telefoongesprekken

Het opnemen van telefoongesprekken door een werkgever mag ten eerste als opname van de gesprekken noodzakelijk is. Een voorbeeld is het verbeteren van de telefonische dienstverlening in een callcenter. Daarnaast moet de werkgever bij het opnemen voldoen aan de algemene voorwaarden voor controle van werknemers uit de [AVG en de UAVG](#).

Verder moet de werkgever werknemers ter plekke informeren dat hij hun telefoongesprekken opneemt. Dat kan bijvoorbeeld met een geluidssignaal bij het begin van de opname. Hij moet dan vooraf aan de werknemers uitleggen dat het signaal betekent dat de opname begint en voor welk doel hij de gesprekken opneemt.

Het is niet voldoende dat een werkgever werknemers bij het in dienst komen eenmalig informeert dat hij hun telefoongesprekken kan opnemen. De werknemers moeten het weten als hij een opname maakt van een gesprek. Daarnaast moet de werkgever degene met wie de werknemer belt vooraf informeren dat het telefoongesprek wordt opgenomen en waarvoor de werkgever de opnamen gebruikt, bijvoorbeeld voor trainingsdoeleinden.

Een werkgever mag telefoongesprekken alleen heimelijk opnemen bij bedreigingen, bommeldingen of als hij een werknemer van strafbaar gedrag verdenkt, zoals het verspreiden van bedrijfsgeheimen. Het stiekem maken van opnames van telefoongesprekken voor begeleiding, beoordeling of training van werknemers is niet toegestaan.

Een werknemer heeft het recht de werktelefoon af en toe te gebruiken voor een privégesprek of om een privébericht te sturen, behalve als daarover andere afspraken zijn gemaakt. De werkgever mag het telefoongebruik controleren bij aanwijzingen dat werknemers misbruik maken van een telefoon op of van de zaak. Daarbij moet hij wel voldoen aan de voorwaarden voor controle van werknemers uit de privacywetgeving.

Stel interne richtlijnen op voor e-mail- en internetgebruik op het werk

Monitoring e-mail en internet op het werk

Aan het gebruiken van e-mail en internet op het werk mag een werkgever voorwaarden stellen. Ook mag hij bepaalde soorten gebruik verbieden. Daarna mag hij controles uitvoeren. Die controles moeten wel voldoen aan de privacywetgeving. De werkgever kan het beste [interne richtlijnen opstellen voor e-mail- en internetgebruik op het werk \(tool\)](#).

Een werkgever kan privégebruik van e-mail en internet onder werktijd niet helemaal verbieden. Werknemers hebben namelijk recht op een bepaalde mate van [privacy op het werk](#). Ze moeten daarbij wel maat houden en letten op de inhoud van e-mails en de inhoud van de websites die ze bezoeken. De werkgever kan bijvoorbeeld steekproefsgewijs monitoren of er sprake is van verboden e-mail- of internetgebruik.

Vermoedt een werkgever misbruik door één of meerdere werknemers, dan mag hij onder bepaalde voorwaarden een specifieke, heimelijke controle uitvoeren naar het gebruik van e-mail en internet door deze werknemer(s). Voor deze controle gelden extra voorwaarden. De werkgever moet bijvoorbeeld het doel bepalen waarvoor hij controleert. Van dat doel hangt af hoe omvangrijk de controle mag zijn en hoe die mag plaatsvinden. Voorbeelden van doelen zijn al eerder genoemd: systeem- en netwerkbeveiliging, beschermen van bedrijfsgeheimen of verminderen van kosten en tijdsverlies.

Controle mailbox werknemer

Een werkgever mag in de mailbox van een werknemer kijken als hij langere tijd afwezig is door bijvoorbeeld ziekte of vakantie. Hierbij mag de werkgever alleen de zakelijke e-mail lezen. Daarnaast mag de werkgever niet meer mails lezen dan strikt noodzakelijk is. De werkgever doet er goed aan werknemers te informeren dat hij tijdens vakantie of ziekte hun zakelijke e-mail kan nalopen.

De werkgever moet werknemers vooraf laten weten dat hij ze controleert op social media

Een werknemer kan zelf onderscheid maken tussen zijn zakelijke mail en privémail. Dat kan hij doen door de privémail in een aparte persoonlijke map op te slaan of door bij privémails 'persoonlijk' in de onderwerpregel van het bericht te zetten.

Sociale media

Een werkgever mag controleren wat een werknemer op sociale media zegt over zijn werk. Hij moet daarvoor dan wel een zogeheten gerechtvaardigd belang hebben. Bovendien mag de werkgever alleen openbare informatie op sociale media nagaan. Hij mag de werknemer dus niet onder druk zetten om hem tot vriend te maken op bijvoorbeeld Facebook of om zijn inlogcodes van een account af te geven. De werkgever moet werknemers vooraf laten weten dat hij ze controleert op social media. Hij kan daarvoor het beste interne richtlijnen opstellen.

Wat controleert de software?

Voor het vaststellen van een gerechtvaardigd belang en de bijbehorende belangenafweging is ook het type software waarmee de werkgever controleert van belang. Hij moet dus helder hebben wat de betreffende software precies 'controleert'. Alleen het meten van de schermtijd is minder ingrijpend dan wanneer de software automatisch om de zoveel tijd screenshots maakt van openstaande pagina's. In de eerste situatie zal de belangenafweging eerder in het voordeel van werkgever kunnen uitvallen.

Monitoren thuiswerk

Voor de privacy-eisen aan een controle maakt het niet uit of een werknemer thuiswerkt of op het werk is. Een werkgever mag een werknemer dus niet intensiever monitoren omdat deze op afstand werkt. Ook moet de werkgever bijvoorbeeld goed kunnen onderbouwen waarom het noodzakelijk is dat hij werknemers controleert tijdens het thuiswerken. Daarnaast moet de werkgever de thuiswerker laten weten dat controles mogelijk zijn voordat hij ermee begint.

De werkgever kan een werknemer op verschillende manieren monitoren als deze thuiswerkt. Dat kan bijvoorbeeld met speciale software die registreert wat de werknemer op zijn computer doet (in- en uitloggen, toetsaanslagen, gebruik van e-mail en internet). Of met software waarmee de werkgever screenshots kan maken of foto's van de thuiswerkplek via de webcam.

Vaak kan een werkgever thuiswerkende werknemers echter ook op andere, minder ingrijpende manieren controleren. Dat kan onder meer door afspraken te maken over wat de werknemer op een dag moet doen en hoe hij zich daarover verantwoordt.

Bij controle in privétijd heeft het privacybelang meestal voorrang

Track & trace-systeem

Bij het plaatsen van een track & trace-systeem, zoals een gps-tracker in een bedrijfswagen, moet de werkgever eveneens een zogeheten gerechtvaardigd belang hebben. Zo'n belang is bijvoorbeeld dat de werkgever wil kunnen nagaan welke auto zich het dichtst bij een klant bevindt, zodat hij deze naar de klant kan sturen.

De werkgever moet de OR om instemming vragen voor het gebruik van een track & trace-systeem. Gaat de OR niet akkoord, dan mag de werkgever het track & trace-systeem niet gebruiken. Ook moet de werkgever aan de werknemer laten weten waarom hij track & trace-systeem gegevens verzamelt, wanneer dit gebeurt en om welke gegevens het gaat.

Bij controle in privétijd heeft het privacybelang meestal voorrang boven het belang van de werkgever. Meestal kunnen werknemers een gps-tracker, black box (registratie ritgegevens) of boordcomputer uitzetten als ze in privétijd de auto van de zaak gebruiken.

Cameratoezicht

Soms mag een werkgever (verborgen) camera's inzetten voor de beveiliging van zijn werknemers en eigendommen. Hij mag de camera-opnames dan echter in principe niet gebruiken om de werknemer aan te spreken of te beoordelen. Als er bijvoorbeeld veel diefstal of fraude op het werk is, mag de werkgever onder strenge voorwaarden een verborgen camera gebruiken voor het monitoren van werknemers. De inbreuk op de privacy van de werknemers van cameratoezicht is wel groot.

Werkgevers kunnen biometrische persoonsgegevens gebruiken voor toegangscontrole, zoals een vingerafdruk of gezichtsscan. Dat mag alleen als dat absoluut noodzakelijk is voor de beveiliging van gebouwen of informatiesystemen. [Dat is niet snel het geval.](#)

De werkgever moet een legitieme reden hebben voor het screenen van nieuwe werknemers

Digitale screening

Met [\(digitale\) screening \(tool\)](#) kunnen werkgevers de betrouwbaarheid van (potentiële) werknemers bekijken, voordat ze deze in dienst nemen of houden. Dat kan heel ingrijpend zijn en niet alles is daarbij toegestaan vanuit de wettelijke privacyregels. De werkgever moet een legitieme reden hebben voor de screening en het screenen moet aantoonbaar noodzakelijk zijn. Verder moet de werkgever de sollicitant of werknemer vooraf en achteraf goed informeren over de screening.

Het gerechtvaardigd belang van een werkgever bij screenen betekent meestal dat hij erop moet kunnen vertrouwen dat de (toekomstige) werknemer integer en betrouwbaar is. Noodzakelijkheid bij screening houdt onder meer in dat de werkgever zijn doel niet met een ander, minder ingrijpend middel kan bereiken. Verder kan de werkgever vanuit goed werkgeverschap rekening houden met [de sollicitatiecode](#). Deze is niet verplicht maar bevordert wel een eerlijke en transparante sollicitatieprocedure.

Goed werkgeverschap

Bij het monitoren en controleren van werknemers moet de werkgever zich op basis van artikel 7:611 BW als een goed werkgever gedragen. Hierbij hoort dat de werkgever de persoonlijke levenssfeer van de werknemer respecteert.

'Toestemming' als juridische grondslag voor het inzetten van een personeelsvolgsysteem is in principe niet geldig. In de arbeidsrelatie tussen werkgever en werknemer kan de werknemer immers geen 'vrijelijke toestemming' geven vanwege de ondergeschiktheidsrelatie tussen werknemer en werkgever. Een uitzondering kan zijn dat de werknemer aantoonbaar kan weigeren zonder enig nadelig gevolg.

Werknemers die zich bekeken voelen zullen eerder apparatuur achteroverdrukken

Eerlijkheid duurt het langst

In de praktijk blijken desktopmonitoring, videobewaking en andere vormen van digitale begluurapparatuur eerder averechts te werken, zo blijkt uit [twee onderzoeken](#). Zo zullen werknemers die zich bekeken voelen, eerder valsspelen bij een test of apparatuur achteroverdrukken. Daarnaast wordt opzettelijk langzaam werken door het digitaal monitoren eerder aangemoedigd dan ontmoedigd.

Hoe meer een werknemer het idee heeft dat hij eerlijk wordt behandeld, hoe meer keuzevrijheid hij ervaart en hoe meer hij zich moreel verantwoordelijk voelt. Volgens de onderzoekers is de toepassing van controle-instrumenten dan ook alleen effectief als de werknemer het gevoel heeft dat hij eerlijk wordt behandeld. Een werkgever moet daarom zorgen voor open communicatie. Het uitleggen van de reikwijdte en het doel van monitoring vergroot de acceptatie bij werknemers volgens de onderzoeken met bijna 70%.

Aandachtspunten voor monitoring

- Het monitoren van werknemers in gevoelige ruimtes zoals toiletten of religieuze ruimtes is niet toegestaan.
- Permanente controle is verboden. Werknemers moeten zich op het werk enigszins vrij kunnen voelen.
- Richtlijnen voor controle en monitoring kan de werkgever bijvoorbeeld opnemen in een personeelsreglement of -handboek. Het kan ook met een privacyverklaring en/of een reglement computer- en internetgebruik.
- Een werkgever mag verwerkte gegevens niet voor een ander doel (gaan) gebruiken. Hij moet de verwerking van gegevens opnemen in een verwerkingsregister om achteraf verantwoording te kunnen afleggen over de manier waarop hij gegevens heeft verwerkt. De AP kan dit controleren en maatregelen tegen een werkgever nemen bij het verwerken van gegevens in strijd met de wet.

Dit is een artikel van de redactie van HR Rendement

HR Rendement is dé informatiebron voor HR-professionals die hun organisatie verder willen helpen. De insteek is: hoe kan een HR-adviseur, HR-medewerker of andere HR-specialist bijdragen aan een beter rendement van personeel en arbeid? HR Rendement behandelt onderwerpen zoals wijzigingen in wet- en regelgeving, ontwikkelingen in het arbeidsrecht, fiscaal voordelige beloningsvormen, arbeidsvoorwaarden, arbeidsomstandigheden, personeelssubsidies en de inzet van HR-instrumenten en personeelsdata.

De onafhankelijke en ervaren redactie van HR Rendement zit bovenop het nieuws en vertelt u als eerste wat deze ontwikkelingen zijn. Altijd in heldere taal en met een praktische insteek, zodat u de informatie direct kunt vertalen naar uw eigen werksituatie. HR Rendement is daarnaast multimediaal. De voor uw vakgebied relevante informatie verschijnt:

- ✓ dagelijks op het digitale platform Rendement Online, waar u onder meer het laatste nieuws, checklists, rekentools, maatwerkbrieven en verdiepingsartikelen tot uw beschikking heeft;
- ✓ wekelijks gebundeld in een e-mailnieuwsbrief;
- ✓ maandelijks in het vakblad HR Rendement, boordevol nieuws en achtergrondartikelen, digitaal en op de mat;
- ✓ tweemaandelijks in een handzaam themadossier: een pocketboekje dat iedere editie een complex onderwerp uitdiept.



Rendement is een succesvolle uitgeverij van met name praktische vakbladen en digitale ondersteuning.

Het assortiment bestaat uit een crossmediaal portfolio: van printuitgaven zoals magazines en themadossiers tot online ondersteuning in de vorm van digitale naslagwerken, e-nieuwsbrieven, een vragenservice en tools.

www.rendementuitgeverij.nl