Privacy op de werkvloer tijdens een pandemie

Reijnen, K.

In het onderwerp ‘privacy op de werkvloer’ is uitgewerkt hoe werkgevers -normaal gesproken- om dienen te gaan met werknemersgegevens conform de regels uit de Algemene verordening gegevensbescherming (AVG). Er kunnen echter bijzondere situaties optreden waardoor er nieuwe vragen ontstaan rondom die regels en de uitwerking van de AVG. Niet te vergeten dat we überhaupt nog bezig zijn met de algehele uitkristallisering van deze wetgeving.
Momenteel hebben we helaas te maken met zo’n bijzondere situatie; er is namelijk sprake van een pandemie. Zoals gezegd roept een bijzondere situatie allerlei vragen op rondom de privacy van werknemers. Bij werkgevers zal het voornamelijk gaan om de vraag of zij gezondheidsgegevens van werknemers mogen verwerken en hoe zij kunnen zorgen dat hun werknemers veilig thuiswerken. Het COVID-19 virus brengt namelijk ook met zich mee dat werkgevers hun organisatie anders moeten inrichten omdat zij moeten anticiperen op de gevolgen van dit virus op de werkvloer.
In dit onderwerp worden daarom de belangrijke punten rondom privacy op de werkvloer tijdens een pandemie behandeld. Zo kunnen werkgevers in deze bijzondere situatie de privacy van werknemers blijven beschermen, maar ook bijdragen aan de bestrijding van de pandemie.
Let op: dit onderwerp is geschreven naar de huidige stand van zaken. De ontwikkelingen gaan snel en we proberen belangrijke wijzigen en nieuws z.s.m. door te voeren. Verder is het raadzaam om het nieuws binnen Opmaat Privacyrecht te volgen, daar komen de belangrijkste ontwikkelingen altijd terecht.

Bijgewerkt tot 8 juni 2020

PRIVACY & COVID-19

Werkgevers zullen nu veel (preventieve) maatregelen willen én moeten treffen ter bestrijding van het COVID-19 virus. De overheid vraagt dit expliciet van werkgevers en werkgevers moeten op grond van de Arbeidsomstandighedenwet *(Arbowet)* hun werknemers een veilige en gezonde werkomgeving bieden. Het komt de werkgever dus toe maatregelen te treffen inzake de werkorganisatie tijdens een pandemie. Daarbij kan gedacht worden aan flexibele werkuren, thuiswerken, uitstel van personeelsfeesten etc. Verder kan (en moet) de werkgever instructies opleggen inzake sociale afstand en hygiëne op de werkvloer.

Zodra deze maatregelen gepaard gaan met verwerking van persoonsgegevens, moeten de bepalingen uit de AVG gerespecteerd worden. De Autoriteit Persoonsgegevens (AP) heeft daarbij benadrukt dat privacy belangrijk is, maar dat de bestrijding van het COVID-19 virus en het redden van levens topprioriteit is. Dit moet dan ook tijdens een pandemie het uitgangspunt zijn. Echter, dit betekent dus niet dat privacy tijdens een pandemie overboord gegooid mag worden. De toezichthouder zal nog steeds ingrijpen wanneer de privacy echt in gevaar is en er kunnen altijd nog

boetes opgelegd worden als blijkt dat een werkgever niet conform de AVG en adviezen van de AP heeft gehandeld, ook tijdens een pandemie.

WAT BEPAALT DE AVG?

Wat bepaalt de AVG

Alle maatregelen ter bestrijding van de pandemie waarbij persoonsgegevens worden verwerkt, dienen te voldoen aan de beginselen uit artikel 5 AVG. Net zoals alle anderen verwerkingen van persoonsgegevens. Deze beginselen worden in andere artikelen nader uitgewerkt.

Bijvoorbeeld: art. 5 lid 1 AVG *(Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (Voor de EER relevante tekst)) bepaalt dat verwerkingen rechtmatig dienen te zijn en dit wordt nader uitgewerkt in* art. 6 AVG *(Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (Voor de EER relevante tekst)). In artikel 6 AVG worden namelijk de rechtsmatigheidsgronden uiteengezet.*

Lees hier *(Regels voor verwerken)* meer over de basisregels voor het verwerken van persoonsgegevens.

Gezondheidsgegevens

Gezondheidsgegevens

Werkgevers zullen tijdens een pandemie voornamelijk vragen hebben over de gezondheid van hun werknemers. Dit zijn bijzondere persoonsgegevens en worden - omdat zij gevoelig van aard zijn- extra beschermd door de wet. In art. 9 lid 1 AVG *(Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (Voor de EER relevante tekst))* is daarom een verwerkingsverbod opgenomen voor de verwerking van deze persoonsgegevens. Alleen als aan een voorwaarde uit lid 2 van dit artikel wordt voldaan én er kan een beroep gedaan worden op een rechtmatigheidsgrond uit art. 6 AVG, mag van dit verbod worden afgeweken.

Lees ook de Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers voor meer algemene informatie over dit onderwerp.

Tijdens een pandemie gelden gewoon de bovengenoemde algemene regels rondom de verwerking van bijzondere persoonsgegevens *(Persoonsgegevens)*. In principe mogen werkgevers dus geen gezondheidsgegevens van werknemers verwerken, behalve als de werkgever zich kan beroepen op een uitzondering.

Voorbeeld 1: In een arbeidsrelatie bestaat er een loondoorbetalingsverplichting bij ziekte. De werkgever moet dan wel weten of een werknemer ziek is (maar hoeft niet te weten wat de werknemer heeft). Dit is een wettelijke verplichting vanuit het arbeidsrecht. Zo heeft de werkgever dus een rechtmatigheidsgrond conform artikel 6 AVG en is er sprake van een uitzondering uit artikel 9 AVG, waardoor de verwerking van gezondheidsgegevens is toegestaan.

Voorbeeld 2: Een werkgever mag in uitzonderlijke gevallen met toestemming van de werknemer gegevens over de aard en oorzaak van een ziekte registeren. Daarbij kan gedacht worden aan de situatie waarin een werknemer epilepsie heeft en collega's hiervan op de hoogte moeten zijn, zodat zij weten wat ze moeten doen als de werknemer een aanval krijgt.

Let op: toestemming gaat bijna nooit op in een arbeidsrelatie. Dit is een uitzondering. Meer lezen hierover kunt u hier (Privacy op de werkvloer).

Werkgevers mogen dus niet:

- vragen naar de gezondheid van werknemers;
- zelf gezondheidstesten bij werknemers afnemen;
- de reden van ziekmelding bijhouden.

Dit betekent niet dat werkgevers niets kunnen en mogen tijdens een pandemie, maar wel dat zij zich ook nu aan de AVG moeten houden of acties kunnen ondernemen waarbij de AVG geen rol speelt.

Werknemers mogen dus wel:

- algemene informatie registeren welke noodzakelijk is tijdens de afwezigheid van de zieke werknemer. Bijvoorbeeld hoe lang de ziekte vermoedelijk gaat duren;
- praten met medewerkers over het virus (maar geen gedeelde gezondheidsgegevens vastleggen of zelf delen);
- een besmette werknemer de toegang tot het kantoor ontzeggen. Dit is noodzakelijk om besmetting te voorkomen. Als de werkgever verder nog preventiemaatregelen wil treffen, moet de identiteit van de besmette werknemer niet worden vrijgegeven. De Arbodienst en/of GGD kunnen - indien nodig - hierbij helpen.

RUIMTE IN DE AVG?

Ruimte in de AVG?

Zoals hierboven gemeld, moet er gewoon worden voldaan aan de regels rondom het verwerken van (bijzondere) persoonsgegevens bij het nemen van maatregelen ter bestrijding van het COVID-19 virus. De European Data Protection Board (EDPB) en de AP zien ook genoeg ruimte voor werkgevers om maatregelen te kunnen treffen tijdens deze crisis én daarbij niet af te doen aan de bescherming van de privacy van werknemers. Zie hieronder een uiteenzetting van hun recente publicaties.

Wat zegt de EDPB?

Wat zegt de EDPB

De EDPB heeft op 19 maart 2020 een verklaring gepubliceerd over de verwerking van persoonsgegevens in het kader van het COVID-19 virus. De EDPB benadrukt daarin dat de AVG geen belemmering vormt voor maatregelen in de strijd tegen het COVID-19 virus, maar dat de verwerkingsverantwoordelijken en verwerkers ook tijdens de crisis erop toe moeten zien dat de privacy van betrokkenen beschermd wordt.

Verder staat in de verklaring dat de AVG voorziet in wettelijke grondslagen voor de verwerking van persoonsgegevens in deze context. De AVG staat volksgezondheidsautoriteiten en werkgevers namelijk toe om persoonsgegevens te verwerken in het kader van een pandemie, maar dan wel overeenkomstig de nationale wetgeving en binnen de daarin gestelde voorwaarden.

De EDPB vermeldt daarbij expliciet voor werkgevers dat de verwerking van persoonsgegevens door werkgevers noodzakelijk kan zijn om te voldoen aan een wettelijke verplichting waaraan de werkgever is onderworpen, zoals verplichtingen met betrekking tot gezondheid en veiligheid op de werkplek, of voor het algemeen belang, zoals de bestrijding van ziekten en andere bedreigingen voor de gezondheid. De AVG voorziet daarbij ook in uitzonderingen op het verbod op de verwerking van bepaalde speciale categorieën persoonsgegevens, zoals gezondheidsgegevens, wanneer dit om redenen van algemeen belang op het gebied van de volksgezondheid nodig is (artikel art. 9 lid 2 sub i AVG *(Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (Voor de EER relevante tekst))*), op grond van het Unierecht of het nationale recht, of wanneer de vitale belangen van de betrokkene moeten worden beschermd (art. 9, lid 2, onder c AVG), aangezien overweging 46 AVG expliciet verwijst naar de bestrijding van een epidemie.

Volgens de verklaring is de verwerking van (bijzondere) persoonsgegevens in deze context dus mogelijk:

- om een wettelijke verplichting te vervullen;
- om redenen van algemeen belang op het gebied van volksgezondheid (op grond van het Unierecht of het nationale recht);
- om vitale belangen te beschermen.

Opmerking met betrekking tot het laatste punt: de AVG verplicht bij het verwerken van bijzondere persoonsgegevens om vitale belangen te beschermen, dat dit alleen mag als er geen toestemming gegeven kan worden. Dit zal op de werkvloer tijdens deze pandemie niet snel het geval zijn. Helaas gaat de EDPB verder ook niet in op het feit dat toestemming in een arbeidsrelatie vrijwel nooit een geldige grondslag is.

De EDPB geeft dus aan dat de AVG voldoende grondslagen en uitzonderingen biedt voor werkgevers om (bijzondere) persoonsgegevens te kunnen verwerken ter bestrijding van de pandemie. Het is echter wel de vraag of nationale wetgeving het

toe laat dat werkgevers zich hier ook echt op kunnen beroepen. Dit zal dan ook per geval bekeken moeten worden.

De EDPB benadrukt verder uitdrukkelijk dat de basisbeginselen van de AVG ook nu in acht genomen moeten worden. Verder moeten maatregelen die zijn geïmplementeerd om de huidige crisis te managen en het onderliggende besluitvormingsproces worden gedocumenteerd.

Vervolgens bevat de verklaring nog een volledige Q&A over COVID-19 en werkgelegenheid.

De Q&A van EDPB

Q: Can an employer require visitors or employees to provide specific health information in the context of COVID-19?

A: The application of the principle of proportionality and data minimisation is particularly relevant here. The employer should only require health information to the extent that national law allows it.

Q: Is an employer allowed to perform medical check-ups on employees?

A: The answer relies on national laws relating to employment or health and safety. Employers should only access and process health data if their own legal obligations requires it.

Q: Can an employer disclose that an employee is infected with COVID-19 to his colleagues or to externals?

A: Employers should inform staff about COVID-19 cases and take protective measures, but should not communicate more information than necessary. In cases where it is necessary to reveal the name of the employee(s) who contracted the virus (e.g. in a preventive context) and the national law allows it, the concerned employees shall be informed in advance and their dignity and integrity shall be protected.

Q: What information processed in the context of COVID-19 can be obtained by the employers?

A: Employers may obtain personal information to fulfil their duties and to organise the work in line with national legislation.

Nationale wetgeving

In de verklaring van de EDPB wordt dus voornamelijk verwezen naar nationale wetgeving. Nederland moet in die gevallen terugvallen op wat er in de UAVG en nationale arbeid-, gezondheid- en veiligheidswetgeving staat.

Wat zegt de AP?

Wat zegt de AP?

De AP heeft op haar website een pagina gewijd aan COVID-19 virus (hier ook corona genoemd) op de werkvloer. Op deze pagina beantwoordt zij belangrijke vragen waar werkgevers mee kunnen zitten tijdens deze pandemie. Zie hieronder.

Mag ik mijn werknemers controleren op corona?

Als werkgever mag u uw personeel niet zelf controleren op corona. Alleen een (bedrijfs)arts mag werknemers controleren. De arts deelt de uitslag vervolgens alleen met de werknemer.

Zieke werknemer

Is de werknemer ziek? Dan kan hij of zij zich op de gebruikelijke manier bij u ziekmelden.

Maatregelen werkvloer

Vermoedt de arts dat uw werknemer het coronavirus heeft? Dan neemt de arts met spoed contact op met de regionale GGD. De GGD kan dan in overleg met u maatregelen treffen voor op de werkvloer.

Instructies RIVM

Het RIVM heeft instructies gegeven hoe met contacten op het werk en met klanten om te gaan. Van alle werkgevers wordt verwacht dat zij de instructies van het RIVM volgen.

En dat zij hun medewerkers hier nadrukkelijk op wijzen. Zorg ervoor dat de instructies van het RIVM in alle talen van uw werknemers beschikbaar zijn.

Mag ik mijn werknemer vragen of hij of zij corona heeft?

Nee, dat mag niet. Als werkgever mag u niet vragen naar de aard en oorzaak van iemands ziekte.

Let op: vertelt uw werknemer uit zichzelf wat hij of zij mankeert? Dan mag u deze informatie niet vastleggen of delen.

Opmerking auteur: Eerder had de AP op haar website nog staan dat het in de zorg wel mag.

Mijn werknemer is positief getest op corona. Moet ik nu iedereen inlichten die met mijn werknemer in contact is geweest?

Nee, dit is niet aan u. Test een (bedrijfs)arts uw medewerker positief op corona? Dan geeft de arts dit door aan de GGD. Is er door contacten van uw werknemer kans op besmetting op de werkplek? Dan treedt een protocol van de GGD in werking. Dat protocol bepaalt welke maatregelen worden genomen.

Opmerking auteur: Op dit vlak geeft de AP een andere toelichting dan de EDPB. Het is raadzaam om de AP te volgen. Echter, als er intern mondeling wordt besproken dat er een COVID-19 besmetting is en dat daardoor bepaalde maatregelen worden doorgevoerd, is er nog geen sprake van een verwerking in de zin van de AVG.

Moet mijn werknemer het aan mij melden als hij of zij corona heeft?

Nee. Uw medewerker hoeft u als werkgever niet te informeren over de aard en oorzaak van zijn of haar ziekte.

Uw werknemer mag dit wel vrijwillig aan u vertellen. Maar let op: u mag deze informatie vervolgens niet vastleggen of delen.

Mag ik mijn zieke werknemer naar huis sturen?

Of u dit mag, kan de AP niet beoordelen. Deze situatie staat namelijk los van de bescherming van persoonsgegevens.

Het hangt ervan af wat wel en niet mag in arbeidsverhoudingen. Hiervoor moet u naar het arbeidsrecht kijken.

UPDATE

Mag ik een werknemer vragen om zijn of haar gezondheid te checken?

Eerder had de AP het volgende antwoord gegeven:

Ja. U mag van uw werknemer verlangen om zijn of haar gezondheid scherp in de gaten te houden. Zeker als uw werknemer niet thuis aan het werk is.

De werknemer zou dit dan onder werktijd zelf kunnen controleren. Bijvoorbeeld door zelf zijn of haar temperatuur te meten.

Het antwoord is echter onlangs veranderd in:

Of u dit mag, kan de AP niet beoordelen. Deze situatie staat namelijk los van de bescherming van persoonsgegevens.

Het hangt ervan af wat wel en niet mag in arbeidsverhoudingen. Hiervoor moet u naar het arbeidsrecht kijken.

UPDATE

Mag ik een werknemer vragen om contact op te nemen met een arts?

Eerder had de AP het volgende antwoord gegeven:

U mag uw werknemer altijd vragen om contact op te nemen met de bedrijfsarts, arbodienst of huisarts voor controle.

Vermoedt de arts dat uw werknemer het coronavirus heeft? Dan neemt de arts met spoed contact op met de regionale GGD. De GGD kan dan in overleg met u maatregelen treffen voor op de werkvloer.

Het antwoord is echter onlangs veranderd in:

Of u dit mag, kan de AP niet beoordelen. Deze situatie staat namelijk los van de bescherming van persoonsgegevens.

Het hangt ervan af wat wel en niet mag in arbeidsverhoudingen. Hiervoor moet u naar het arbeidsrecht kijken.

Opmerking auteur: elders op de website van de AP zegt de AP wel nog steeds: 'Natuurlijk mag uw werkgever wel van u verlangen dat u uw gezondheid zelf goed in de gaten houdt. En contact opneemt met de bedrijfsarts zodra dat nodig is.'

Temperaturen tijdens corona

Temperaturen tijdens corona

Een veel besproken onderwerp rondom privacy op de werkvloer in temperaturen tijdens corona. Daarom heeft de AP een pagina toegevoegd aan het dossier privacy op de werkvloer over dit onderwerp. De AP benadrukt: naast dat niet zeker is of hiermee coronabesmettingen kunnen worden opgespoord, is temperaturen niet

zomaar toegestaan. Meestal verwerkt de werkgever hiermee namelijk medische gegevens en dat valt onder de AVG.

Update

Om dit te verduidelijken legt de AP op haar website uit waarom de AVG geldt en wanneer de AVG niet geldt.

Waarom geldt de AVG?

De AVG geldt in deze situatie omdat u niet alleen iemands temperatuur meet, maar u vervolgens ook iets doet met dit medische gegeven. U meet immers niet voor niets. Dit wordt namelijk meestal geregistreerd of doorgegevens om vervolgens een actie te kunnen ondernemen.

Wanneer geldt de AVG niet?

De AVG geldt niet als alleen de temperatuur wordt afgelezen en daar verder niets mee gebeurt. Dus als de temperatuur niet wordt geregistreerd en ook niet in een geautomatiseerd systeem terechtkomt. Aflezen op zichzelf valt dus niet onder de AVG.

Maar let op: ook al is de AVG niet van toepassing, de inbreuk op iemands privacy kan toch groot zijn. En ook de bescherming van andere grondrechten, zoals de integriteit van het lichaam, kan nadrukkelijk in het geding zijn. De AP kan hier echter niet tegen optreden.

Vragen van werkgevers & werknemers over temperaturen tijdens corona

De AP geeft ook antwoord op enkele vragen.

Q: Mag mijn werkgever mijn temperatuur opnemen tijdens de coronacrisis?
A: Nee. Het opmeten van uw temperatuur door uw werkgever is ook tijdens de coronacrisis ten strengste verboden. Uitsluitend een (bedrijfs)arts mag gezondheidstests doen. En uw gezondheidsgegevens verwerken

Q: Mag ik als werkgever mijn werknemers temperaturen als zij daarvoor toestemming geven?
A: Nee, dat mag niet. U mag geen medische gegevens van uw werknemers verwerken. En dus hun temperatuur niet opmeten. Zelfs als uw werknemers of uw OR uitdrukkelijke toestemming geven om te temperaturen, mag u dit niet doen.

Q: Mag ik mijn medewerkers verplichten om hun eigen temperatuur op te nemen of mee te werken aan uitsluitend temperaturen?
A: Wilt u uw medewerkers zelf hun temperatuur laten opmeten? Of wilt u alleen hun temperatuur (laten) meten, zonder daar iets mee te doen (dus de temperatuur niet registreren of automatisch verwerken)?

Of u dit mag, kan de Autoriteit Persoonsgegevens (AP) niet beoordelen. Deze situatie staat namelijk los van de bescherming van persoonsgegevens. Het hangt ervan af wat wel en niet mag in arbeidsverhoudingen. Hiervoor moet u naar het arbeidsrecht kijken.

Q: Mag ik mijn medewerkers verplichten thuis te werken, zich ziek te melden of de bedrijfsarts in te schakelen?

A: Laat u de temperatuur van uw medewerkers opmeten? Bijvoorbeeld door henzelf? En wilt u dat uw medewerkers zelf ingrijpen als hun temperatuur niet goed is? Of u dit mag, kan de Autoriteit Persoonsgegevens (AP) niet beoordelen. Deze situatie staat namelijk los van de bescherming van persoonsgegevens. Het hangt ervan af wat wel en niet mag in arbeidsverhoudingen. Hiervoor moet u naar het arbeidsrecht kijken.

Opmerking auteur

De AP heeft ondertussen regelmatig haar antwoorden en informatie gewijzigd én zal dit naar verwachting blijven doen. We proberen dit onderwerp zo snel mogelijk te actualiseren indien nodig, maar we verwijzen u door naar de pagina van de AP voor de volledige antwoorden op deze vragen en alle informatie over temperaturen tijdens corona. Dit zodat u altijd de meest actuele informatie kan raadplegen. U vindt de pagina hier.

AP benadrukt bijzondere situatie

De AP wijkt in de basis niet af van wat we gewend zijn, maar geeft in haar antwoorden wel aan dat er ruimte is voor werkgevers om het virus te bestrijden.

Verder heeft de AP in een nieuwsbericht benadrukt dat zij ruim baan geven aan de broodnodige initiatieven om de capaciteit van de zorg op niveau te krijgen. Zo klopte een zorgorganisatie bij de AP aan met een plan om mensen die tot een paar jaar geleden in de zorg werkten, te benaderen om hen tijdelijk weer als arts of verpleegkundige in te zetten. Dat lieten organisaties (ex-werkgevers) door een tussenpersoon doen en zij vroegen zich af of dit wel mag. De AP heeft met ze meegedacht over een goede oplossing. De AP zegt daarbij: *‘Privacy moet goede zorg nooit in de weg zitten, zeker nu niet.'*

Prioriteit bestrijden COVID-19

Prioriteit is nu het bestrijden van het COVID-19 virus en het redden van levens, aldus de AP. In deze bijzondere situatie is het dus denkbaar dat meer mogelijk is, mits dit noodzakelijk is om de volksgezondheid te beschermen én privacy gewaarborgd blijft.

Conclusie

Conclusie

De AVG staat werkgevers niet in de weg om maatregelen te nemen tijdens een pandemie. Dit wordt bevestigd door de EDPB en de AP.

Dit betekent niet dat werkgevers opeens van alles mogen vastleggen omdat we te maken hebben met een bijzondere situatie. Werkgevers moeten ook nu de AVG in acht blijven nemen. Het is dus belangrijk dat werkgevers belangenafwegingen blijven maken als zij nieuwe verwerkingen willen gaan doen ter bestrijding van de pandemie, de risico’s afwegen en zich houden aan het Unierecht en nationale wetgeving.

Verder moet niet vergeten worden dat er ook veel ondernomen kan worden zonder (extra) persoonsgegevens te verwerken. Niet elke maatregel zal dus betrekking hebben op een verwerking van persoonsgegevens in de zin van de AVG. Dit betekent niet dat er dan geen inbreuk gemaakt kan worden op de privacy van personen (grondrecht) of rekening gehouden moet worden met het arbeidsrecht. Ondanks dat de AVG dan geen bescherming biedt, kan een inbreuk alsnog onrechtmatig zijn of een schending van arbeidsrechtelijke regel zijn. Kijk dus altijd naar het gehele plaatje.

Voorbeeld maatregel zonder verwerken persoonsgegevens
Werkgevers leggen nieuwe hygiënemaatregelen op. Daarvoor hoeven geen (extra) gegevens verwerkt te worden, maar het is wel erg efficiënt tijdens een pandemie.

Opmerking auteur

Opmerking auteur: alle informatie in dit onderwerp is op 10 mei 2020 geüpdatet aan de hand van de wijzigingen van de AP in haar informatie en antwoorden op haar website. Een belangrijke toevoegen is dat de AP nu ook benadrukt dat in sommige gevallen zij niet kan beoordelen of iets mag of niet. Dit aangezien de situatie dan los staat van de AVG. Eerder kon u in dit onderwerp lezen dat ik mijn bedenkingen had bij antwoorden van de AP, omdat er in veel situaties helemaal geen persoonsgegevens worden verwerkt in de zin van de AVG. En dat ik het bijzonder vond dat de AP niet verwees naar het arbeidsrecht. Gelukkig komt de AP daar nu op terug en geeft zij aan dat er ook naar het arbeidsrecht gekeken moet worden.

MAATREGEL: THUISWERKEN

Thuiswerken

Een maatregel om de verspreiding van het COVID-19 virus te voorkomen is het laten thuiswerken van werknemers. Het RIVM en de overheid vragen ook van werkgevers, voor zover mogelijk, om werknemers vanaf huis te laten werken. Het opvolgen van deze richtlijnen valt onder de zorgplicht van de werkgever om te zorgen voor een veilige en gezonde werkomgeving.

Bij thuiswerken spelen twee belangrijke privacyaspecten een rol:

1. Veilig thuiswerken. Er bestaat namelijk een risico dat de beveiliging minder goed op orde is dan op het werk zelf. Dit brengt bijvoorbeeld met zich mee dat de kans op datalekken toeneemt.
2. De privacy van de thuiswerkende werknemer.

Veilig thuiswerken

Veilig thuiswerken

Werkgevers zullen moeten zorgen dat zij beleid opstellen rondom thuiswerken. Dit zodat de werkplek goed ingericht kan worden (arbeidsrechtelijke verplichting), maar ook zodat werknemers weten welke maatregelen genomen moeten worden om de privacy te blijven waarborgen.

Voorbeelden

Enkele voorbeelden van maatregelen voor in het thuiswerkbeleid zijn:

- Scherm afsluiten bij toiletbezoek/pauzes.
- Zoveel mogelijk zorgen dat familieleden niet kunnen meeluisteren tijdens videogesprekken.
- Documenten die je normaal aan elkaar overhandigd nu beveiligd mailen.

Aanbevelingen

Aanbevelingen

De AP en het Nationaal Cyber Security Centrum (NCSC) hebben aanbevelingen gedaan voor veilig thuiswerken. Het is raadzaam voor werkgevers om deze op te volgen en tevens te verwerken in beleid.

Tips van de AP voor veilig thuiswerken:

- Werk in een beveiligde omgeving.
- Bescherm gevoelige documenten.
- Wees voorzichtig met het gebruik van (video)chatdiensten.
- Let op phishingmails.

Aanbevelingen van het NCSC voor organisaties:

- Zorg voor de benodigde (netwerk)capaciteit om het grotere aantal thuiswerkers te kunnen bedienen. Denk hierbij zowel aan de IT-infrastructuur als aan de telecominfrastructuur.
- Maak een beoordeling welke medewerkers op kantoor aanwezig dienen te zijn voor de ondersteuning van de IT-voorzieningen die nodig zijn voor thuiswerken.
- Bedenk welke aanpassingen mogelijk nodig zijn voor uw incident respons plannen bij een beperkte aanwezigheid van medewerkers.
- Dwing het gebruik van een veilige verbinding naar het bedrijfsnetwerk af met bijvoorbeeld met een Virtual Private Network (VPN) of andere veilige thuiswerkoplossing.
- Zorg dat thuiswerkmogelijkheden getest en geüpdatet zijn.
- Stel eventueel extra monitoring in op uw applicaties die kritiek zijn voor thuiswerken.
- Maak zoveel mogelijk gebruik van multifactorauthenticatie (MFA) voor toegang tot uw bedrijfsnetwerk en dwing sterke wachtwoorden af.
- Installeer de meest recente updates voor hard- en software.
- Zorg dat uw medewerkers bewust zijn van phishing omtrent COVID-19/ het Coronavirus en dat bekend is hoe zij dit moeten melden. Houd rekening met een mogelijke toename van meldingen omtrent phishingmails en valse e-mails.
- Zorg dat uw organisatierichtlijnen up-to-date zijn en bekend zijn bij de medewerkers omtrent informatiebeveiliging inclusief het (thuis)gebruik van hard- en software en het eventuele gebruik van privé IT-voorzieningen.

Communicatiemiddelen

Communicatiemiddelen

Momenteel wordt er veel gebruik gemaakt van tools om bijvoorbeeld werkoverleg te voeren of presentaties te houden. Bijvoorbeeld via Zoom, Skype of FaceTime. De AP waarschuwt daarbij dat organisaties voorzichtig moeten zijn met het gebruik daarvan. Dit is niet gek, want er worden veel persoonsgegevens gedeeld/verwerkt als er gebruik wordt gemaakt van zo'n middel.

Tips bij het gebruik van communicatiemiddelen:

- Kies zo veel mogelijk voor een communicatiemiddel waarbij zekerheid is over de beveiliging. Bijvoorbeeld gewoon de telefoon.
- Als een organisatie een alternatief moet kiezen, doe ‘onderzoek’ naar de privacy risico’s en maak gemotiveerd een keuze. Controleer dus in ieder geval de privacyverklaring van de leverancier en de veiligheid van de verbinding.
- Stel –indien mogelijk- de tool gebruiksvriendelijk in.
- Weiger niet-relevante cookies.
- Sluit verwerkersovereenkomsten waar nodig.
- Verwijder data zo snel mogelijk.
- Probeer zo min mogelijk (gevoelige) gegevens te delen.
- Vraag instemming rondom het gebruik en informeer klanten over het gebruik van nieuwe communicatiemiddelen.
- Update de eigen privacyverklaring.

Keuzehulp privacy bij videobel-apps

De AP heeft bij 13 veelgebruikte videobel-apps gekeken naar de belangrijkste privacyaspecten. Zoals welke gegevens de app verzamelt, wat de app daarmee doet en of de communicatie beveiligd is. Aan de hand daarvan heeft de AP een keuzehulp gemaakt welke kan bijdragen aan een keuze maken voor een geschikt middel.

Onderzoek door IBD

Onderzoek IBD

De informatiebeveiligingdienst (IBD) heeft van gemeenten veel vragen gekregen over videoconferencing tools. Daarom hebben zij onderzoek gedaan en verschillende adviezen op een rijtje gezet. Deze zijn niet alleen voor gemeenten interessant, maar voor iedere organisatie die deze tools wil gebruiken. De IBD heeft daarbij ook quickscan gedaan op de beveiligingsmaatregelen van veel verschillende tools.

De IBD is onderdeel van de VNG en ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). Teksten van de IBD-website mogen worden overgenomen, daarin mogen echter geen veranderingen worden aangebracht. Om deze reden vindt u hieronder een kopie van het door de IBD gedeelde bericht.

Videobellen is in deze tijd een welkome aanvulling op alle andere kanalen die we al gebruiken om met elkaar te communiceren nu het persoonlijke contact tot een minimum beperkt moet worden. Videobellen is niets meer dan een stream van beeld en geluid daar waar we voorheen voornamelijk alleen geluid van de telefoon gebruikten. De beveiligingsmaatregelen zijn ook niet anders dan die we nu al gebruiken voor de communicatie via mail, geluid en chatten gebruiken. Het NCSC heeft in 2017 een factsheet “Kies een berichtenapp voor uw organisatie” geschreven die ook goed toepasbaar is op tools voor videobellen.

Let op dat er altijd een zekere mate van beveiligings- en privacyrisico is bij het gebruik van dergelijke tools. Het risico moet u afwegen tegen het doel en de omstandigheden. Videochatten zal bijna nooit het medium zijn voor het uitwisselen van (zeer) vertrouwelijke informatie.

Dit advies gaat in op technische en juridische maatregelen, de factor mens is echter een hele belangrijke. Zeker in deze periode van thuiswerken is het goed mogelijk dat gezinsleden van de deelnemers delen van het gesprek meekrijgen, screenshots en video-opnames kunnen worden gedeeld, etc. Dat vereist een zekere mate van vertrouwen in de deelnemers.

Daarom tip 1:

Besef wat u deelt! Houd rekening met het feit dat wat u bespreekt in principe openbaar zou kunnen worden.

Een generieke aanpak voor het beoordelen van een app voor videobellen kan zijn:

- Kies een app die altijd bij alle deelnemers werkt.
- Kies een app die een unieke ID genereert die maar voor 1 persoon te gebruiken is.
- Kijk ook naar open source, enkele alternatieven:
    - https://jitsi.org
    - https://callaba.io/
    - https://whereby.com/
- Enkele betaalde alternatieven:
    - https://zoom.us
    - https://24sessions.com
    - https://teams.microsoft.com/
    - https://www.webex.com

Denk voor de risicoafweging aan de volgende punten:

- De keuze voor een app is afhankelijk van het doel van de vergadering en welke (persoons)gegevens er worden gedeeld in zo'n vergadering. Ook kunnen organisaties waar u mee gaat vergaderen andere eisen stellen aan de vergaderomgeving.
- De risico's die te maken hebben met Amerikaanse cloudleveranciers hebben we op onze website al op een rijtje gezet
- Controleer of de videoapp/aanbieder tenminste over de volgende maatregelen beschikt:
    a. End-to-end encryptie
    b. Hashing van wachtwoorden

c. AES 256 bit TLS encryptie bij voorkeur

d. SAML 2.0

e. Unieke vergader id's om vergaderingen af te schermen

f. Compliant aan AVG/GDPR of EU privacyshield

g. Bij voorkeur: Datacenter in EU, verwerking in EU

h. Gecertificeerd: ISAE 3402 type 2, SOC 2 type 2, ISO 27001

i. Client over HTTPS

j. Lage latency

k. Indien gewenst: on-premise mogelijkheden met eventueel cloud back-up

- Controleer de bovenstaande beveiligingseisen (zie hiervoor de quickscan).
- Controleer of de aanbieder van de app voldoet aan de AVG/GDPR en of er privacyvriendelijke instellingen aanwezig zijn, zoals de keuze om persoonsgegevens alleen op te slaan in de EU of een optie om een adresboek van de organisatie niet te uploaden naar de server. Lees ook de aanbevelingen van het NCSC en de Autoriteit Persoonsgegevens over videochatdiensten.
- Als (een deel van) de opslag of andere verwerking van persoonsgegevens door de aanbieder buiten de EER plaatsvindt, controleer dan of er een adequaatsheidsbesluit is genomen door de Europese Commissie, of (bij Amerikaanse partijen) of er een Privacyshield certificaat is. Verifieer het certificaat op https://www.privacyshield.gov/list.
- Zorg ervoor dat de omgang met en inrichting van de tool zoveel mogelijk privacyvriendelijk gebeurt: zet (attention)trackingfuncties uit en neem het gesprek niet op.
- Wijs iemand in de groep aan die in de gaten houdt of hetgeen besproken wordt ook besproken kan en mag worden (let in het bijzonder op persoonsgegevens).
- Creëer een intern of besloten adresboek/contactlijst van de organisatie om te gebruiken in de app.
- Maak medewerkers bewust van de omgeving wanneer u de tool gebruikt. Denk om zaken zoals wie kan meeluisteren, of er (gevoelige) persoonsgegevens in beeld zijn tijdens de videoconference en het afsluiten van de videoconference na afronding van het gesprek.
- Stel een toegangsbeperkende maatregel (bijv. pincode) in voor het gebruik van de app of kies een app die een random nummer gebruikt voor een uniek gesprek.
- Gebruik alleen apps waarbij end-to-end encryptie ingeschakeld is.

- Wordt de app ook mobiel gebruikt, zorg dan bij voorkeur voor een MDM/MAM oplossing voor het beheer van de mobiele devices.
- Wordt de toepassing ook gebruikt voor klantcontact, zorg dan voor een verificatieprocedure, zodat u kunt vaststellen dat u ook zeker weet dat de ander is wie hij zegt dat hij is.

Bron: Informatiebeveiligingsdienst, 25 maart 2020

DPIA?

DPIA?

Normaal gesproken moet een organisatie een DPIA uitvoeren bij het gebruik van nieuwe technologieën. Dit is ook het geval als werkgevers besluiten gebruik te gaan maken van nieuwe tools om bijvoorbeeld te kunnen videobeelden. De punten waar hierboven naar wordt verwezen zijn belangrijk om mee te nemen in zo een DPIA. Aangezien we nu te maken hebben met een bijzondere situatie en er snel geanticipeerd moet worden op deze situatie, kan een DPIA lastig zijn. Een verkort onderzoek kan daarom voor nu ook voldoende zijn. De AP geeft aan dat er sowieso onderzoek gedaan moet worden naar de privacy risico's. Vergeet dit dus echt niet ondanks alle hectiek.

Let op: Het is raadzaam om later alsnog een volledige DPIA uit te voeren.

Privacy van de thuiswerkende werknemer

Privacy thuiswerkende werknemer

Ook thuiswerkende werknemers hebben recht op privacy. Dit betekent dat werkgevers hun werknemers niet zomaar mogen controleren. Dit is alleen toegestaan als wordt voldaan aan de AVG en de UAVG. Ook tijdens een pandemie.

Voorbeeld: Werkgevers zullen benieuwd zijn naar de productiviteit van werknemers. Echter, e-mails mogen inhoudelijk niet zomaar bekeken worden. Een minder ingrijpende actie kan zijn om te kijken naar de hoeveelheid e-mails die verstuurd zijn. Verder is een goed controlemiddel het gebruik maken van een werklijst. Hierbij is redelijkheid nog steeds een vereiste, maar kan een werkgever wel vragen in brede zin waar de werknemer dus zijn of haar tijd aan heeft besteed. Niet op de minuut natuurlijk en vooral geen wc-breaks laten opnemen.

Alles over controle van werknemers kunt u vinden op de website van de AP.