*Mr. drs. M. Jansen*[1]



# Privacy en corona vanuit het perspectief van de ondernemer

*Ondernemingsrecht* 2020/XV

**In dit artikel wordt een inleiding gegeven op het privacyrecht. Vervolgens worden de volgende vier thema's behandeld: bezoekersregistratie, ziekmeldingen en de zorgplicht van de werkgever, monitoring en thuiswerken. Aan de hand van deze vier thema's worden specifieke privacyrechtelijke aandachtspunten (kort) besproken. Specifieke aandacht is er voor de ruimte die de Autoriteit Persoonsgegevens sinds enige tijd biedt aan werkgevers in tijden van corona. De auteur signaleert dat die ruimte voor de praktijk (te) beperkt is.**

## 1. Inleiding

De coronacrisis roept bij de ondernemer diverse privacygerelateerde vragen op. In dit artikel sta ik bij enkele van die thema's kort stil. Allereerst zet ik kort de privacywetgeving uiteen om vervolgens in te gaan op de specifieke aandachtspunten en kernvragen die in ondernemingen rondom corona zullen leven. Met dit artikel is zeker geen volledig uitputtende verhandeling beoogd. Thema's die meer in de publieke sector spelen, laat ik rusten. Het juridisch kader rondom de privacy is verspreid over diverse wetten. Ik zal de kern hierna kort toelichten.

## 2. Juridisch kader

### 2.1 *AVG en UAVG*

#### 2.1.1 *Algemene privacywetgeving*

De belangrijkste privacyregels worden sinds 25 mei 2018 gegeven door de combinatie van Europese AVG (verordening 2016/679[2]) en de Nederlandse Uitvoeringswet AVG (UAVG). Deze zijn in Nederland zowel binnen als buiten de werkingssfeer van het Unierecht van toepassing.[3]

#### 2.1.2 *Breed toepassingsbereik*

De AVG en UAVG zijn van toepassing op iedere "verwerking" van "persoonsgegevens", mits die verwerking geautomatiseerd plaatsvindt of de persoonsgegevens in een bestand zijn opgenomen of bestemd zijn in een bestand te zijn opgenomen.[4] Persoonsgegevens zijn alle gegevens die al dan niet met enige moeite[5] naar een persoon herleid kunnen worden.[6] Het begrip "verwerken" is zo breed gedefinieerd dat hiervoor ook gelezen kan worden: ieder werkwoord dat voor de woorden 'van persoonsgegevens' kan staan.[7] Van een bestand is reeds sprake wanneer de persoonsgegevens "*zijn gestructureerd volgens specifieke criteria die het in de praktijk mogelijk maken deze gegevens gemakkelijk terug te vinden voor een later gebruik ervan*".[8]

#### 2.1.3 *Beginselgebaseerde wetgeving en procedurevoorschriften*

De kern van de AVG en de UAVG is dat bij de verwerking van persoonsgegevens de beginselen van artikel 5 AVG in acht worden genomen. Dit zijn de beginselen van rechtmatigheid, eerlijkheid, doelbinding, minimale gegevensverwerking, juistheid en relevantie, beperkte opslagduur en integriteit en vertrouwelijkheid. Het is van belang zich dit beginselkarakter goed te realiseren; het privacyrecht bevat – behoudens bij de verwerking van bijzondere persoonsgegevens en de procedurevoorschriften (daarover beide hierna meer) – weinig absolute ("harde") regels. Dat maakt ook dat de wetgeving aan veel interpretatie onderhevig is.

Verder mogen gegevens alleen worden verwerkt indien daarvoor een (of meer) rechtsgrond(en) uit artikel 6 AVG aanwezig is. Een veelvoorkomend misverstand is dat met de komst van de AVG voor iedere verwerking toestemming van de betrokkene is vereist. Toestemming is echter een van de zes mogelijke rechtsgronden en dient bij voorkeur te worden vermeden.

De AVG schrijft verder voor dat organisaties allerlei procedurevoorschriften dienen na te leven. Die zien veelal op het borgen van een rechtmatige verwerking van persoonsgegevens (uitvoeren DPIA, aanstellen F-G, etc.). Deze werk ik hier niet verder uit, doch hier kom ik waar passend in hoofdstuk 3 op terug.

De AVG kent de betrokken verder diverse rechten toe, maar deze zal ik ook niet verder bespreken.

De AVG bevat ten slotte een uitgebreide regeling omtrent handhaving. Het komt er op neer dat bij nationale kwesties de lokale toezichthouder bevoegd is, terwijl bij grensoverschrijdende kwesties het coördinatie- en coherentieme-

1 Mark Jansen is advocaat IT- en privacyrecht te Arnhem. De definitieve versie van dit artikel zal verschijnen in het themanummer 'Ondernemingsrecht in tijden van corona'.

2 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).

3 Artikel 3 lid 2 jo. lid 1 sub a UAVG.

4 Artikel 2 lid 1 AVG.

5 Hof van Justitie 19 oktober 2016, ECLI:EU:C:2016:779, r.o. 48.

6 Artikel 4 sub 1 AVG.

7 Artikel 4 sub 2 AVG.

8 Hof van Justitie 10 juli 2018, ECLI:EU:C:2018:551, r.o. 62.

chanisme moet worden gevolgd door de toezichthouders. De toezichthouders kunnen allerlei maatregelen treffen, waaronder boetes opleggen tot 20.000.000 euro of 4% van de wereldwijde omzet.

2.1.4 *Bijzondere persoonsgegevens*

Rondom bijzondere persoonsgegevens geldt een strenger regime. De verwerking van deze gegevens is verboden, behoudens wettelijke uitzonderingen of de toestemming van betrokkene.

Onder bijzondere persoonsgegevens worden verstaan persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, alsmede genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid en gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.[9]

Meer specifiek worden onder "gegevens over gezondheid" verstaan "*persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven*".[10]

Op grond van artikel UAVG zijn er enkele uitzonderingen op het verbod gezondheidsgegevens te verwerken. Zo mogen gezondheidsgegevens onder meer worden verwerkt door werkgevers indien dat noodzakelijk is voor de re-integratie of begeleiding van werknemers bij ziekte.[11] Voor verzekeraars,[12] scholen en reclasseringsinstellingen[13] gelden een vergelijkbaar beperkte uitzonderingen op het verbod. En uiteraard mogen hulpverleners in de gezondheidszorg gezondheidsgegevens verwerken, maar ook slechts voor zover noodzakelijk voor hun taak.[14] De Autoriteit Persoonsgegevens (AP) heeft op 23 februari 2016 beleidsregels uitgevaardigd over de interpretatie van de regels omtrent de verwerking van ziekmeldingen door werkgevers.[15] Die beleidsregels zijn zeer streng te noemen. Zo wordt in de beleidsregels benadrukt dat werkgevers de werknemer nergens naar mogen vragen en bevatten de beleidsregels een limitatieve lijst met gegevens die bij een ziekmelding mogen worden verwerkt. De beleidsregels benadrukken verder dat de werkgever ook niet naar andere gegevens dan die limitatieve lijst bij de werknemer mag vragen.

2.1.5 *Uitleg tegen het licht van grondrechten*

Het is vaste rechtspraak dat de AVG en UAVG moeten worden uitgelegd tegen het licht van grondrechten, waaronder het grondrecht op de bescherming van de relationele privacy.[16] Daarbij kan uit verschillende grondrechtencatalogi worden geput; het Europese Hof van Justitie heeft reeds geoordeeld dat de rechten die in het EU Handvest worden toegekend op gelijke wijze moeten worden uitgelegd als de vergelijkbare rechten die in het EVRM staan.[17]

2.2 ***Grondrechten***

Het meest in het oog springende grondrecht in dit kader is artikel 8 van het Europees Verdrag voor de Rechten van de Mensen (EVRM). Op grond van dit artikel heeft eenieder het recht op "*respect voor zijn privéleven, zijn familieen gezinsleven, zijn woning en zijn correspondentie*". Het Europees Hof voor de Rechten van de Mens interpreteert het begrip privéleven breed[18] en past het ook al vele decennia ook buiten overheidsverhoudingen toe. Hierbij valt te denken aan de vele procedures over onrechtmatige publicaties,[19] maar ook aan procedures over het monitoren van gedrag op de werkvloer[20] of procedures tegen bedrijven die aan grootschalige gegevensverzameling doen.[21]

Naast dat de grondrechten langs de band van (de interpretatie van) de AVG van belang zijn (zie hiervoor), kunnen deze in veel gevallen ook rechtstreeks worden ingeroepen. Artikel 8 EVRM is immers een "een ieder verbindende bepaling" in de zin van artikel 93 en 94 Grondwet. In de Nederlandse praktijk wordt dan ook veelvuldig een beroep gedaan op artikel 8 EVRM en de op grond daarvan door het EHRM gewezen rechtspraak. Dat gebeurt zowel rechtstreeks als ter nadere invulling van andere juridische begrippen (zoals onrechtmatige daad, goed werkgeverschap, etc.).

2.3 ***Medezeggenschapsrecht***

Op grond van artikel 27 van de Wet op de ondernemingsraden (WOR) behoeft de ondernemer instemming van de ondernemingsraad voor elk door hem voorgenomen besluit tot vaststelling, wijziging of intrekking van een pri-

9 Artikel 9 AVG.
10 Artikel 4 sub 15 AVG.
11 Artikel 30 lid 1 sub b UAVG.
12 Artikel 30 lid 3 sub b UAVG.
13 Artikel 30 lid 2 sub a en sub b UAVG.
14 Artikel 30 lid 3 sub a UAVG.
15 Autoriteit Persoonsgegevens, "*De zieke werknemer. Beleidsregels voor de verwerking van persoonsgegevens over de gezondheid van zieke werknemers*", 23 februari 2016, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_de_zieke_werknemer.pdf.
16 Zie o.m. AVG-considerans overweging 1, 4, 10; Hoge Raad 9 september 2011, ECLI:NL:HR:2011:BQ8097; HvJEU 20 mei 2003, ECLI:EU:C:2003:294, r.o. 68-69.
17 HvJEU 9 november 2010, ECLI:EU:C:2010:662, r.o. 52.
18 EHRM 4 december 2008, S. AND MARPER v. THE UNITED KINGDOM, ECLI:CE:ECHR:2008:1204JUD003056204
19 Zie bijvoorbeeld de diverse arresten over Von Hannover, zoals EHRM 07 februari 2012, ECLI:CE:ECHR:2012:0207JUD004066008.
20 Zoals EHRM 05 september 2017, ECLI:CE:ECHR:2017:0905JUD006149608
21 Zoals EHRM 27 juni 2017, ECLI:CE:ECHR:2017:0627JUD000093113.

vacybeleid[22] en voorzieningen voor monitoring[23] van werknemers. Inzake monitoring wijs ik specifiek op dat de instemmingsplicht niet alleen speelt rondom voorzieningen die daadwerkelijk gebruikt gaan worden voor monitoring, maar ook op voorzieningen die daar geschikt voor zijn. Voor bijvoorbeeld veel thuiswerkfaciliteiten geldt dat deze geschikt zijn voor monitoring, nu deze gebruikt kunnen worden om te zien of en zo ja welk werk er door de werknemer via de faciliteit wordt verricht (daarover meer in par. 3).

## 3. Gevolgen van de coronacrisis

Nu de coronacrisis in volle omvang losbarst, spelen er enkele kwesties vanuit privacyrechtelijk perspectief. Deze zal ik hierna kort bespreken.

### 3.1 *Corona en bezoekers aan het bedrijf*

Veel bedrijven nemen maatregelen om besmetting en verspreiding binnen het bedrijf te voorkomen. Zolang die de maatregelen niet specifiek zien op het gedrag of eigenschappen van een bepaald individu, staat de privacywetgeving daaraan niet in de weg. Zo is er bijvoorbeeld niets op tegen om – in generieke zin – te faciliteren dat mensen hun handen wassen of dat bezoekers hun temperatuur opmeten.

Het wordt echter anders indien die maatregelen zich vervolgens ook toespitsen op het individu. Om bij de genoemde voorbeelden te blijven: zodra wordt geregistreerd of een bezoeker zijn handen wast, of een bezoeker zijn temperatuur opmeet of wat de temperatuur van de bezoeker was, is onmiskenbaar sprake van de verwerking van persoonsgegevens. En dat roept ogenblikkelijk de vraag op wat de noodzaak van een dergelijke "handenwasdatabase" zou zijn. Die vraag is nog niet eenvoudig te beantwoorden, maar vermoedelijk wreekt hier zich dat het bedrijf zich min of meer de taak van de gezondheidsautoriteiten aan het toe-eigenen is, hetgeen niet aan bedrijven is.

Voor het vastleggen van de gemeten temperatuur is het antwoord in ieder geval evident: daar is sprake van de verwerking van gezondheidsgegevens.[24] Het verwerken van dergelijke gezondheidsgegevens is verboden, behoudens een wettelijke uitzondering of toestemming. Toestemming vragen aan de betrokkene om de gegevens vast te leggen zal veelal problematisch zijn. Toestemming veronderstelt immers dat de betrokkene een keuze heeft (dat hij ook "nee" kan zeggen). Die ruimte tot weigering maakt toestemming een ongeschikt grondslag in dergelijke context. Behoudens wettelijke uitzonderingen is dit dus niet toegestaan.

Bedrijven dienen er bij bezoekersregistratie ook erop bedacht te zijn dat er mogelijk indirecte administraties ontstaan die gevoelig van aard kunnen zijn. Zo zou het verschil tussen een lijst genodigden en een lijst aanwezigen in feite een lijst van zieken kunnen opleveren, zeker wanneer bij de deur iedereen met een te hoge temperatuur wordt geweigerd. Bedrijven doen er goed aan die verschillenanalyse (dus) niet te maken.

### 3.2 *De werkgever en ziekmeldingen*

Veel werkgevers zien – bijvoorbeeld in het kader van goed werkgeverschap – een rol voor zichzelf weggelegd bij ziekmeldingen wegens corona. Dit ziet dan zowel op de zorg voor de zieke medewerker, als de vrees voor besmettingen bij de overige werknemers. Zoals hiervoor uiteengezet, is het kader rondom ziekmeldingen zeer streng te noemen. Volgens de AP mag slechts een limitatieve hoeveelheid gegevens worden verwerkt voor een beperkt aantal doeleinden. Goed werkgeverschap en zorg richting andere werknemers is zeker geen door de AP erkend doel. Dat laatste komt waarschijnlijk omdat de AP zich slechts als hoeder van de privacy ziet.

De AP is echter sinds enige tijd gedeeltelijk "om" gegaan. Op de website is nu een afzonderlijke sectie opgenomen getiteld "Corona op de werkvloer".[25] Nog steeds wordt benadrukt dat een werkgever niet zelf een werknemer mag (laten) testen. Ook wordt nog steeds benadrukt dat de werkgever niets over de aard van de ziekte mag vastleggen, ook als de werknemer die informatie zelf in vrijheid geeft.[26] Nieuw is echter onder meer dat een werkgever volgens de AP een vermoedelijk zieke werknemer naar huis mag sturen. Dat is echt een majeure draai, nu de AP in de eerdere beleidsregels benadrukte dat het niet aan de werkgever is om aan diagnose te doen. Verder vindt de AP dat van een werknemer verlangd mag worden dat deze periodiek zijn eigen gezondheid in de gaten houdt. Ook dat is opmerkelijk te noemen, nu de AP tot op heden juist altijd benadrukte dat voor een oordeel over de gezondheid de bedrijfsarts moet worden ingeschakeld. De AP wijst er ten slotte op dat het niet aan de werkgever is om maatregelen te treffen indien een werknemer corona heeft, nu in dat geval de GGD conform protocol actie zal ondernemen.

22 Artikel 27 lid 1 sub k WOR: "*een regeling omtrent het verwerken van alsmede de bescherming van de persoonsgegevens van de in de onderneming werkzame personen*".

23 Artikel 27 lid 1 sub l WOR: "*regeling inzake voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen*".

24 Vergelijk de beslissing van de Autoriteit Persoonsgegevens in de Uniperkwestie over het voornemen alcoholtests af te nemen: iedere meting waaruit gezondheidsconclusies zijn af te leiden is een (verboden) verwerking van bijzondere persoonsgegevens. Autoriteit Persoonsgegevens, Rapport definitieve bevindingen z2015-00971, november 2016, gepubliceerd op: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/01_rapport_db_uniper_def.pdf.

25 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/corona/corona-op-de-werkvloer

26 Het is vast beleid van de AP dat een werknemer geacht wordt niet in vrijheid hierover tegenover de werkgever te kunnen verklaren.

In de praktijk gaan veel bedrijven overigens verder dan de AP op dit punt toestaat, bijvoorbeeld door actief aan medewerkers te vragen of ze klachten hebben en de antwoorden op die vragen vast te leggen. Ook zijn er mogelijk werkgevers die actief contact zoeken met de GGD bij vermoedens van corona. In de visie van de AP is het echter niet aan werkgevers om maar iets te vragen, laat staan vast te leggen over de aard van een ziekte. Doorgifte aan de GGD is dan al helemaal niet aan de orde (want er ligt immers niets vast). De vraag is of hier geen sprake is van een lacune in de wetgeving. Enerzijds is een aan beroepsgeheim gebonden arts nota bene verplicht om, ondanks dat beroepsgeheim, een vermoeden van corona te melden.[27] De ratio daarvan zal zijn dat het belang van de collectieve volksgezondheid zwaarder weegt dan het individuele belang op privacy. Terwijl anderzijds de werkgever diezelfde, voor het collectieve belang eveneens relevante informatie, niet eens mag vastleggen. En hoewel de bedrijven ongetwijfeld goede bedoelingen zullen hebben, stellen ze zich met hun verantwoordelijke opstelling in beginsel bloot aan handhaving door de AP.

In de rest van Europa wordt overigens een deels wisselende lijn gevolgd. De European Data Protection Board (EDPB) – vrij vertaald: de gezamenlijke Europese toezichthouder – hebben op 19 maart 2020 een gezamenlijke verklaring over corona uitgebracht.[28] Het is een vrij generiek en breed *statement*, dat in algemene zin benadrukt dat privacyregels niet in de weg hoeven te staan aan de bestrijding van corona, maar dat tegelijkertijd de bescherming van de privacy wel geborgd moet blijven. De EDPB wijst erop dat de AVG afwijkingen naar nationaal recht toestaat. De Belgische toezichthouder volgt een enigszins met de AP vergelijkbare lijn, zij het dan in België het opnemen van temperatuur nog niet wordt beschouwd als een verwerking van persoonsgegevens.[29] In Frankrijk wordt benadrukt dat het niet is toegestaan systematisch medische gegevens van werknemers te verzamelen of te verwerken en dat bij een coronamelding slechts mag worden vastgelegd dat een melding is gedaan en welke maatregelen zijn getroffen (dus beperkt tot niet-medische gegevens).[30] In Italië wordt een vergelijkbaar strenge benadering gekozen en wordt gesteld dat het niet aan werkgevers is om initiatieven op het gebied van de volksgezondheid te nemen.[31] Volgens het Duitse beleid is er daarentegen veel meer ruimte om op grond van de zorgplicht van een werknemer gegevens te verwerken en vervolgens preventieve maatregelen te nemen.[32] De Engelse toezichthouder ICO benadrukt dat ze een pragmatische en redelijke toezichthouder is die het belang van publieke gezondheid zwaar weegt bij de interpretatie van de privacywet en de keuzes al dan niet handhavend op te treden.[33] Ook stelt de ICO dat het redelijk is aan mensen te vragen of ze een verdacht land hebben bezocht of symptomen genieten, maar dat het zeker niet altijd noodzakelijk is ook veel gegevens vast te leggen.[34] Van een uniforme toepassing van het privacyrecht in de EU kan dus bepaald niet worden gesproken. Dat maakt het voor ondernemingen met grensoverschrijdende activiteiten lastig om de privacyregels uniform toe te passen.

### 3.3 *Corona en andere vormen van monitoring*

In de vorige paragrafen stipte ik al aan dat uitgebreidere vormen van bezoekers- of ziekteadministraties privacyrechtelijk lastig liggen. In lijn daarmee kan al helemaal lastig van bezoekers, werknemers of anderen worden verlangd dat zij bijvoorbeeld een app op hun telefoon installeren of op andere wijze hun gezondheid op systematische wijze door bedrijven in de gaten laten houden. Voorop staat dat bedrijven veelal geen rechtvaardiging voor de verwerking van de bijzondere (namelijk medische) gegevens zullen hebben bij dergelijke vormen van monitoring. Ieder plan van een dergelijke strekking zal daarop in de regel al afstuiten. Daar komt nog eens bij dat het niet is toegestaan om zonder toestemming van de betrokkene via internet gegevens in of op zijn randapparatuur aan te passen of uit te lezen.[35] Laatstgenoemde verbod volgt uit wat veelal de 'cookiewet' wordt genoemd (die dus over veel meer dan cookies gaat).

Strikt genomen kan van de betrokkene toestemming worden gevraagd om zowel het verwerkingsverbod uit de AVG als de 'cookiewet' op te heffen, maar toestemming is alleen geldig indien deze echt in vrijheid is gegeven en dat zal bij monitoring veelal niet het geval zijn (alleen al om-

27 Artikel 22 Wet publieke gezondheid.

28 EDPB, "*Statement on the processing of personal data in the context of the COVID-19 outbreak*", 19 maart 2020, gepubliceerd op: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf.

29 Gegevensbeschermingsautoriteit, "COVID-19 en de verwerking van persoonsgegevens op de werkvloer", gepubliceerd op: https://www.gegevensbeschermingsautoriteit.be/covid-19-en-de-verwerking-van-persoonsgegevens-op-de-werkvloer.

30 Commission Nationale de l'Informatique et des Libertés (CNIL), „*Coronavirus (COVID-19): les rappels de la CNIL sur la collecte de données personnelles*", gepubliceerd op: https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles.

31 Garante per la Protezione dei dati personali, "Coronavirus: Garante Privacy, no a iniziative "fai da te" nella raccolta dei dati. Soggetti pubblici e privati devono attenersi alle indicazioni del Ministero della salute e delle istituzioni competenti", gepubliceerd op: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9282117.

32 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, „Datenschutzrechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie', gepubliceerd op: https://www.bfdi.bund.de/DE/Datenschutz/Themen/Gesundheit_Soziales/GesundheitSozialesArtikel/Datenschutz-in-Corona-Pandemie.html?nn=5216976.

33 Information Commisionar's Office, "Data protection and coronavirus", gepubliceerd op: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/data-protection-and-coronavirus/.

34 Information Commisionar's Office, "Data protection and coronavirus: what you need to know", gepubliceerd op: https://ico.org.uk/for-organisations/data-protection-and-coronavirus/.

35 Artikel 11.7a Telecommunicatiewet.

dat monitoring een bepaalde gezagsrelatie impliceert). Ook iedere vorm van dienstverlening waarbij toestemming wordt 'geruild' tegen (betere) dienstverlening stuit hierop af. Het is dus bijvoorbeeld niet toegestaan om klanten alleen te aanvaarden onder voorwaarde dat ze medische gegevens prijsgeven, of hen op beter niveau te bedienen wanneer ze tot een dergelijke 'uitruil' bereid zijn.

### 3.4 *Corona en thuiswerken*

Veel bedrijven schakelen, al dan niet vanwege overheidsadviezen, zo veel mogelijk over op thuiswerken. Bij thuiswerken worden allerlei verschillende soorten faciliteiten gebruikt, uiteenlopend van technieken voor op afstand inloggen tot faciliteiten voor videobellen of online bestanden delen. Bij thuiswerken zijn vanuit privacy-optiek diverse aandachtspunten in acht te nemen. Deze aandachtspunten gelden in principe altijd. Ik constateer echter dat een deel in de praktijk wat minder aandacht lijkt te krijgen onder druk van de urgentie die uit de coronacrisis voortvloeit.

Het is bij thuiswerkfaciliteiten van groot belang dat kritisch wordt getoetst of de inzet daarvan veilig is. Indien een onveilige techniek of inrichting wordt gebruikt, kwalificeert dat – gelet op de hele brede definitie van wat veelal kortweg een 'inbreuk' (soms ook wel 'datalek') wordt genoemd[36] – vermoedelijk op zichzelf al als een (vermoedelijk meldingsplichtig) datalek (de beveiliging is immers niet langer geborgd).[37] Laat staan dat de risico's op het daadwerkelijk uitlekken van gegevens bij onveilige technieken natuurlijk fors toeneemt (in welk geval een melding vermoedelijk verplicht is). Die onveiligheid kan zowel in de gebruikte techniek als in de toepassing in de praktijk gelegen zijn. Zo zullen veel thuiswerkplekken (lang) niet zo goed beveiligd zijn als de werkplekken op kantoor.[38] Tijdens de coronacrisis worden die thuiswerkplekken echter opeens wel structureel gebruikt. Het risico op missers neemt dan toe. Bedrijven die op stel en sprong overschakelen op thuiswerken kunnen zich op dit punt dus lelijk in de voet schieten.

Naast dat de voorziening zelf veilig moet zijn, is het ook zaak te borgen dat deze op veilige wijze gebruikt wordt. Zo is het van belang de werknemer goed voor te lichten over de risico's en hen van duidelijke voorschriften te voorzien. Is bijvoorbeeld werken op de laptop in het park via onbeveiligde Wifi in uw organisatie toegestaan of niet? Het monitoren op veilig gebruik van de IT-voorzieningen – door bijvoorbeeld actieve analyse van de onderliggende logboeken – is op zichzelf overigens vanuit privacyrechtelijk optiek gerechtvaardigd, mits het maar proportioneel gebeurt en de OR daarvoor toestemming heeft gegeven (zie ook volgende alinea).[39]

Een ander aandachtspunt bij thuiswerken is dat voorzieningen die geschikt zijn voor monitoring van gedrag van werknemers aan de ondernemingsraad (OR) ter goedkeuring moeten zijn voorgelegd. Veel thuiswerkvoorzieningen – zoals van afstand inloggen op kantoor, software om samen aan bestanden te werken, etc. – zijn (in ieder geval potentieel) geschikt om werknemers te monitoren. Een eventueel in de haast uitgerolde voorziening zal dus eigenlijk met net zoveel haast nog langs de OR moeten worden geloodst. Let er ook op dat een weliswaar in het verleden door de OR goedgekeurde thuiswerkvoorziening mogelijk thans in deze crisis heel anders gebruikt wordt. De vraag is of dan nog wel kan worden volgehouden dat voor het huidige gebruik toestemming van de OR is verkregen.

In lijn met het voorgaande punt wijs ik erop dat bij systematische en grootschalige controle en monitoring van werknemers er op grond van regelgeving van de AP een voorafgaande gegevensbeschermingseffectbeoordeling moet worden uitgevoerd.[40] De AP is op grond van artikel 35 lid 4 AVG bevoegd tot het opstellen van dergelijke gedelegeerde regelgeving. Hoge risico's die tijdens de DPIA zijn geïdentificeerd en die niet kunnen worden gemitigeerd, moeten aan de AP worden voorgelegd.[41] Er zal dus waarschijnlijk ook in alle haast een DPIA moeten worden uitgevoerd. Zowel op het niet verrichten van een dergelijke DPIA, als op het niet voorleggen van resterende hoge risico's, staat een maximale boete van € 10.000.000 of 2% van de wereldwijde omzet.[42]

Het is verder van belang dat thuiswerkfaciliteiten niet worden gebruikt (aangegrepen) om medewerkers opeens op meer indringende wijze te monitoren of anderszins te volgen. Medewerkers mogen immers op de werkvloer, en ook als die werkvloer thuis is, de redelijke verwachting hebben dat hun werkgever de privacy respecteert. Die redelijke verwachting wordt ingekleurd door alle omstandigheden van het geval, waaronder hetgeen eerder aan de werknemer kenbaar is gemaakt. De werknemer mag dus verwachten dat hij bij thuiswerken niet anders of strenger in de gaten wordt gehouden dan regulier, tenzij uiteraard dit reeds vooraf kenbaar is gemaakt. Het lijkt echter bij veel beroepen lastig te rechtvaardigen een medewerker bij thuiswerken intensiever te monitoren dan bij werken op kantoor.

36 Artikel 4.12 AVG: "*inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens*".

37 Artikel 33 AVG.

38 Velen zullen blij zijn als ze thuis überhaupt al ongestoord kunnen werken…

39 Overweging 49 considerans AVG.

40 "Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA)" verplicht is", *Staatscourant* 2019, 64418.

41 Artikel 36 lid 1 AVG.

42 Artikel 83 lid 4 AVG.

Het Nationaal Cyber Security Centrum (NCSC) wijst er in een recente publicatie ook op dat bedrijven er goed aan doen hun plannen rondom bedrijfscontinuïteit te herzien, omdat de beschikbaarheid van thuiswerkfaciliteiten nu onder de kritieke bedrijfsprocessen valt. Dit zal bij de meeste bedrijven tot op heden niet het geval zijn geweest.[43]

Ten slotte zal het contract met de leverancier(s) van de thuiswerkfaciliteit(en) moeten voldoen aan alle in artikel 28 AVG genoemde eisen. Wordt hier niet aan voldaan, dan zal het gebruik van de dienst privacyrechtelijk al snel onrechtmatig zijn. Dat is niet alleen juridisch, maar ook publicitair onwenselijk. Zo was recent veel in het nieuws dat de in deze coronacrisis opeens veelgebruikte applicatie Zoom gegevens met o.m. Facebook zou delen.[44] Verder is het uiteraard zaak de contracten ook overigens op redelijkheid te toetsen, ook in crisistijd.

## 4. Ten slotte

Ik heb kort enkele aandachtspunten op een rij gezet rondom corona vanuit privacyrechtelijk perspectief. Met name de draai van de AP valt op: anders dan voorheen krijgt de werkgever nu een klein beetje ruimte om de gezondheid van zijn werknemers in de gaten te houden. De draai is echter nog zo beperkt dat deze voor veel bedrijven vermoedelijk nog niet volstaat. Het is in dat kader ook opmerkelijk dat voor artsen een meldplicht van corona bestaat, terwijl voor bedrijven het in feite verboden is een melding van een vermoeden van coronabestemming te doen (nu het doen van die melding een verboden registratie impliceert). Mogelijk dat op de langere termijn de wetgeving op dat punt zal worden gewijzigd. Voor het overige is het toch ook wel veel 'business as usual', in die zin dat ook voor en na de coronacrisis het zaak is goed en vooral op structurele wijze bezig te zijn met privacy- en cyberrisico's.

43 Nationaal Cyber Security Centrum, Factsheet "Uw thuiswerkfaciliteiten zijn nu onmisbaar", gepubliceerd op: https://www.ncsc.nl/documenten/publicaties/2020/april/1/factsheet-uw-thuiswerkfaciliteiten-zijn-nu-onmisbaar.

44 Business Insider, "*Zoom is being sued for allegedly handing over data to Facebook*", gepubliceerd op: https://www.businessinsider.com/zoom-sued-allegedly-sharing-data-with-facebook-2020-3.