Covid-19

In de strijd tegen de Covid-19 epidemie staan we allen achter het allesoverheersende doel om de volksgezondheid van onze burgers te beschermen. Maar zelfs in deze bijzondere periode is het belangrijk dat de beginselen van gegevensbescherming worden nageleefd.

Wij wijzen er nogmaals op dat het beschermen van gegevens geen belemmering vormt voor de strijd tegen de verspreiding van het virus. De privacybeginselen maken het mogelijk om een goed evenwicht te vinden tussen de verschillende belangen die op het spel staan.

Om die reden wil de Autoriteit een paar tips geven zodat het evenwicht bewaard blijft tussen de bescherming van de persoonlijke levenssfeer en de bescherming van de volksgezondheid.

Adviezen rond COVID-19

Het Kenniscentrum van de GBA heeft meerdere adviezen uitgebracht bettreffende ontwerpen van normatieve teksten inzake COVID-19. Ons Algemeen Secretariaat heeft ook adviezen over gegevensbeschermingseffectbeoordelingen (“DPIA”) verstrekt. U vindt ze allemaal opgelijst op de pagina "Adviezen rond COVID-19".

Covid-19 op de werkvloer

Naar aanleiding van de uitbraak van COVID-19 ontving de Gegevensbeschermingsautoriteit recent een aantal terugkerende vragen betreffende de preventieve maatregelen die door bedrijven en werkgevers worden genomen ter voorkoming van de verdere verspreiding van het virus en de voorwaarden waaronder persoonsgegevens - en in het bijzonder gezondheidsgegevens - in dit verband mogen worden verwerkt.

Overeenkomstig artikel 20, 2° van de wet van 3 juli 1978 rust op de werkgever de verplichting “als een goed huisvader te zorgen dat de arbeid wordt verricht in behoorlijke omstandigheden met betrekking tot de veiligheid en de gezondheid van de werknemer”. In uitvoering van deze bepaling treffen vele werkgevers dan ook preventiemaatregelen. De vraag rijst evenwel hoe deze

verplichting zich verhoudt tot het recht van de werknemer op bescherming van zijn privéleven en persoonsgegevens.

Het komt de werkgever uiteraard toe een aantal preventiemaatregelen te treffen inzake werkorganisatie (flexibele werkuren, telewerk, uitstel personeelsfeesten, …) evenals sensibilisering inzake sociale afstand en hygiëne op de werkvloer (zie website FOD Werkgelegenheid, Arbeid en Sociaal Overleg). Van zodra te nemen preventiemaatregelen echter gepaard zouden gaan met een verwerking van persoonsgegevens, moeten ook de bepalingen van de Algemene Verordening Gegevensbescherming (hierna: "AVG") gerespecteerd worden.

Volksgezondheid is voor ons van het allergrootste belang en preventie en recht op bescherming van persoonsgegevens zijn niet tegenstrijdig. We bevelen wel aan om de instructies van de bevoegde overheden - onder meer de FOD Volksgezondheid - na te leven zodat alle genomen maatregelen evenredig zijn. Zo wordt zowel een goede levenshygiëne als een goede "gegevenshygiëne" verzekerd! In antwoord op de recent gestelde vragen brengt de Gegevensbeschermingsautoriteit hieronder enkele algemene principes inzake gegevensbescherming in herinnering en beantwoordt zij een aantal veelgestelde vragen.

Rechtmatigheid van de verwerking (artikelen 6 en 9 AVG)

Ook in het kader van het nemen van preventieve gezondheidsmaatregelen geldt als algemeen principe dat elke verwerking van persoonsgegevens dient te voldoen aan de voorwaarden van artikel 6.1 AVG en gesteund moet zijn op één van de in dit artikel vermelde rechtmatigheidsgronden.

In dit verband dient er in het bijzonder op te worden gewezen dat in deze fase en op basis van de laatste informatie gepubliceerd door de FOD Volksgezondheid met betrekking tot COVID-19 geen reden bestaat voor een ruimere of systematische toepassing van de rechtmatigheidsgrond vervat in artikel 6.1, d) AVG ("noodzaak van de verwerking voor de bescherming van de vitale belangen van de betrokkene of andere natuurlijke personen") in het kader van het nemen van preventiemaatregelen door bedrijven en werkgevers.

Dit geldt des te meer voor de verwerking van gezondheidsgegevens, waarvoor artikel 9 AVG in principe een verwerkingsverbod voorschrijft. Er dient op te worden gewezen dat bedrijven en werkgevers zich voor de verwerking van deze categorie van persoonsgegevens uitsluitend kunnen beroepen op artikel 9.2, i) AVG indien zij handelen in uitvoering van uitdrukkelijke richtlijnen opgelegd door de bevoegde overheden. Verder dient de beoordeling van de risico's voor de gezondheid bovendien niet te worden uitgevoerd door de bedrijven en werkgevers maar door de arbeidsgeneesheer, die bevoegd is voor de opsporing van besmettingen en voor het informeren van de werkgever en de personen die in contact kwamen met de besmette persoon.

Deze informatie wordt door de bedrijfsarts verstrekt op basis van de artikel 6.1, c) en 9.2, b) AVG (verwerking ter uitvoering van een arbeidsrechtelijke verplichting).

Preventiemaatregelen en de algemene beginselen inzake persoonsgegevensverwerking

Bij het verwerken van persoonsgegevens in het kader de tenuitvoerlegging van “COVID-19”-preventiemaatregelen dienen naast de voormelde AVG-bepalingen bovendien de algemene beginselen inzake gegevensverwerking te worden gerespecteerd.

In het bijzonder dienen maatregelen die een verwerking van persoonsgegevens inhouden het proportionaliteitsbeginsel en het beginsel van minimale gegevensverwerking in acht te nemen (artikel 5.1, c) en e) AVG).

Zoals bij elke gegevensverwerking mag immers slechts de minimaal noodzakelijke hoeveelheid gegevens worden verwerkt om het vooropgestelde doel te bereiken.

Verder dienen bedrijven transparant te zijn betreffende de genomen maatregelen en hun werknemers en bezoekers afdoende te informeren betreffende de verwerkingsdoeleinden en de bewaartermijn van de in dit kader verzamelde persoonsgegevens (artikel 5.1, a) AVG).

Tot slot moeten ook de nodige beveiligingsmaatregelen in acht worden genomen ter bescherming van de te verwerken persoonsgegevens (artikel 32 AVG).

Mag ik een realtime infrarood camera in de onthaalruimte van mijn bedrijf plaatsen waarmee de lichaamstemperatuur van mijn werknemers kan gemonitord worden?

Neen, dit mag niet. De lichaamstemperatuur van een persoon is een gezondheidsgegeven. De verwerking van gezondheidsgegevens is krachtens artikel 9.1 AVG verboden tenzij een wet hierop een uitzondering maakt. Bij gebrek aan een dergelijke wettelijke uitzondering (bijvoorbeeld een CAO) mag een verwerkingsverantwoordelijke niet de lichaamstemperatuur meten van de werknemers door middel van geavanceerde elektronische meettoestellen zoals koortsscanners en hittecamera’s. Zie ook onze aparte FAQ over dit topic.

Mag ik de werknemers en bezoekers van mijn bedrijf verplichten een vragenlijst in te vullen om na te gaan of zij symptomen van COVID-19 vertonen, of zij zich tijdens de

afgelopen 14 dagen in een risicogebied bevonden en of zij recent in contact kwamen met personen die positief testten op COVID-19?

Neen, dit mag niet. De AVG is van toepassing op de registratie van persoonsgegevens in de vragenlijst.

Een organisatie kan bezoekers of werknemers nooit verplichten tot het invullen van een dergelijke vragenlijst. Deze vragen peilen naar de gezondheidssituatie van de bezoeker of werknemer, waardoor u gezondheidsgegevens zou verwerken.

De verwerking van gezondheidsgegevens is krachtens artikel 9.1 AVG verboden tenzij een wet hierop een uitzondering maakt of de betrokkene vrije toestemming verleent. In de relatie tussen werknemer en werkgever is de toestemming van de werknemer zelden vrij omdat een werknemer grote druk kan ondervinden om toe te stemmen.

Het invullen van de vragenlijst is bijgevolg uitsluitend mogelijk indien de werknemer of de bezoeker in alle vrijheid kan weigeren om de vragenlijst in te vullen zonder nadelig gevolgen te ondervinden (bijv. geen toegang krijgen tot de werkplaats). Bijgevolg kan u een bezoeker of werknemer niet verplichten om deze vragenlijst in te vullen.

Mag mijn werkgever mij verplichten om een coronatest te ondergaan?

Neen, dit mag niet. Een werkgever kan niet louter vanuit zijn patronaal gezag een dergelijke test verplicht opleggen aan het personeel. Dit raakt immers aan de fysieke integriteit van de werknemers. Zonder wettelijke basis mag een werknemer niet worden gedwongen om zich te laten testen. De Autoriteit benadrukt echter dat het soms van groot belang kan zijn dat een personeelslid zich laat testen, zoals bijvoorbeeld in de medische sector.

Mag een werkgever zijn personeel verplichten om een armband te dragen die moet helpen om de regels inzake social distancing na te leven op de werkvloer, risicocontacten te registreren en de locatie van de werknemers te observeren.

Situatie 1: de armband ondersteunt op anonieme wijze enkel het houden van een veilige afstand (zgn. “social distancing”)

Ja, dit mag.

Wanneer de armband louter een signaal uitstuurt in geval een tweede armband zich binnen een vooraf bepaalde perimeter bevindt, ziet de Autoriteit geen probleem: de twee armbanden meten dan enkel de afstand, en als die te klein wordt (< 1.5 m) gaat er een alarm af om de betrokkenen te verwittigen. Er is geen enkele link mogelijk met een identificeerbaar persoon. Dit is toegelaten.

Situatie 2: de armband ondersteunt niet alleen het houden van een veilige afstand (zgn. “social distancing”), maar slaat ook locatiegegevens op.

Neen, dit mag niet.

In dit geval is de AVG van toepassing, omdat (locatie)gegevens van identificeerbare personen worden gebruikt.

Aangezien hier sprake is van een opslag van informatie of het verkrijgen van toegang tot opgeslagen informatie in de eindapparatuur (hier: de armband) van de werknemer, zijn artikel 5 (3) van de e-privacyrichtlijn en artikel 129 van de Belgische wet van 13 juni 2005 betreffende de elektronische communicatie van toepassing. Dit betekent dat de toestemming van de werknemer noodzakelijk is om dit systeem uit te rollen.

Deze toestemming moet vrij zijn zoals voorgeschreven door artikel 7.4 van de AVG. In de relatie tussen werknemer en werkgever is de toestemming van de werknemer zelden vrij omdat een werknemer druk kan ondervinden om toe te stemmen. Het dragen van de armband is dus niet mogelijk omdat de werknemer dit niet in alle vrijheid kan weigeren zonder enig nadelig gevolg te ondervinden (bijv. geen toegang krijgen tot de werkplaats).

Mag ik in mijn winkel een camera installeren die op basis van artificiële intelligentie een waarschuwing stuurt naar een winkelbediende wanneer de bezoeker geen mondmasker draagt?

Neen, dit mag meestal niet.

De camera die de bezoeker van de winkel filmt voert een verwerking van persoonsgegevens uit, zelfs wanneer de camerabeelden uitsluitend lokaal en heel kortstondig worden bewaard (real-time detectie).

Artikel 5 van de AVG schrijft voor dat een verwerking van persoonsgegevens steeds proportioneel moet zijn: toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor het nagestreefde doeleinde.

De winkel zal moeten aantonen dat deze detectie via camerabeelden de enig efficiënte maatregel was en dat minder privacy-intrusieve oplossingen (zoals visuele controle door winkelbediende) ontoereikend waren. Behoudens uitzonderlijke omstandigheden is de Autoriteit van mening dat deze manier van detectie in het merendeel van de situaties disproportioneel is.

Mag ik op de werkplaats een camera installeren die op basis van artificiële intelligentie een waarschuwing stuurt naar de werkgever wanneer een werknemer geen mondmasker draagt?

Neen, dit mag meestal niet.

De camera die de werknemers filmt voert een verwerking van persoonsgegevens uit, zelfs wanneer de camerabeelden uitsluitend lokaal en heel kortstondig worden bewaard (real-time detectie).

Artikel 5 van de AVG schrijft voor dat een verwerking van persoonsgegevens steeds proportioneel moet zijn: toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor het nagestreefde doeleinde. Ook de collectieve arbeidsovereenkomst nr. 68 inzake camerabewaking op de werkplaats herhaalt dit principe.

De werkgever zal moeten aantonen dat de detectie via camerabeelden de enig efficiënte maatregel was en dat minder privacy-intrusieve oplossingen (zoals visuele controle door toezichthoudend personeel) ontoereikend waren. Behoudens uitzonderlijke omstandigheden is de Autoriteit van mening dat deze manier van detectie in het merendeel van de situaties disproportioneel is.

Indien de werkgever kan aantonen dat de verwerking proportioneel is, moet deze de bepalingen van de collectieve arbeidsovereenkomst nr. 68 inzake camerabewaking op de werkplaats naleven.

Mag een bedrijf of werkgever in het kader van de voorkoming van de verdere verspreiding van het virus de namen van besmette personen/werknemers bekendmaken?

Op grond van het vertrouwelijkheidsbeginsel (artikel 5.1, f) AVG) en het beginsel van de minimale gegevensverwerking (artikel 5.1, c) AVG) mag een werkgever de namen van betrokken personen niet zomaar binnen het bedrijf bekendmaken. Ook proportionaliteit is een belangrijk na te leven uitgangspunt bij het verwerken van (al dan niet medische) persoonsgegevens. Met het oog op bijvoorbeeld de preventie van verdere verspreiding mag de werkgever uiteraard wel

andere werknemers op de hoogte brengen van een besmetting, zonder vermelding van de identiteit van de betrokken perso(o)n(en).

Het is inderdaad in de meeste gevallen niet nodig (of zelfs wenselijk) om een naam te vermelden, omdat dit ook een stigmatiserend effect zou kunnen hebben.

De naam van de besmette persoon mag wel gecommuniceerd worden aan de arbeidsgeneesheer of de bevoegde overheidsdiensten.

Kan een werkgever eisen dat zijn werknemers in het geval van een Covid-19-besmetting dit melden aan hem om de veiligheid van de andere werknemers en derden te kunnen waarborgen?

Neen. Werknemers zijn wel verplicht door de Arbeidsovereenkomstenwet en de Welzijnswet om zorg te dragen voor de veiligheid en gezondheid van andere werknemers en derden. Daarbij hebben werknemers ook de verplichting om zich te onthouden van al wat schade kan berokkenen aan andere werknemers en derden. Deze verplichtingen zorgen er niet voor dat de werkgever van zijn werknemers kan eisen dat ze hem in geval van een Covid-19-besmetting rechtstreeks informeren.

Een werknemer die een Covid-19-besmetting heeft opgelopen kan dit vrijwillig aan zijn werkgever melden. Dit machtigt de werkgever echter niet om deze informatie te verwerken. Deze informatie is een persoonsgegeven in het licht van de AVG en mag in principe niet verwerkt worden. Zo mag de werkgever de identiteit van de besmette werknemer niet meedelen aan de medewerknemers. De werkgever mag daarentegen wel op grond van de vrijwillige mededeling de medewerknemers op de hoogte stellen van een besmetting met het oog de preventie van een verdere verspreiding van het virus, maar hier mag de identiteit van de betrokken werknemer niet bekendgemaakt worden.

Wanneer de werkzaamheden van de werknemers intensieve menselijke contacten inhouden kan een werkgever wel aan de werknemers vragen om Covid-19-besmettingen vertrouwelijk te melden aan de arbeidsgeneesheer.

Welke informatie mag ik aan een werknemer vragen die omstandigheidsverlof (klein verlet) vraagt om zich te laten vaccineren?

Wanneer een werknemer een klein verlet aanvraagt om zich te laten vaccineren mag u als werkgever alleen de informatie opvragen die strikt noodzakelijk is om de reden (vaccinatie tegen

Covid-19) en het tijdstip te controleren. De werkgever mag daarom vragen om de bevestiging van vaccinatie-afspraak te tonen.

De werkgever mag echter geen kopie nemen van deze bevestiging en mag evenmin registreren welke werknemers zich op welk ogenblik lieten vaccineren. Het volstaat om, na de controle van de bevestiging van de afspraak, de afwezigheid te boeken als klein verlet.

Meer informatie kan u vinden in het advies 25/2021 van het Kenniscentrum.

Koorts meten in het kader van de strijd tegen COVID-19

De GBA stelt vast dat in het kader van de heropstart van het maatschappelijk en economisch leven verwerkingsverantwoordelijken zoeken naar technologische oplossingen om aan de ingang van hun gebouwen individuen te detecteren die koorts ontwikkelen om te voorkomen dat zij die gebouwen zouden betreden en dit om verdere besmettingen binnen de gebouwen te voorkomen. Zij zien het opzetten van een dergelijk toegangsbeleid als hun taak (namelijk om de veiligheid en gezondheid van de betrokken personen te beschermen).

Dergelijke temperatuurafname geschiedt dan via een klassieke thermometer, via digitale koortsscanners gericht op het voorhoofd van de betrokkene of via geavanceerde hittecamera-systemen.

De GBA begrijpt dat de huidige situatie beproevend is voor iedereen maar herinnert eraan dat het temperaturen van natuurlijke personen onder de AVG valt indien die handeling op zich of naderhand aanleiding geeft tot een verwerking van persoonsgegevens.

In dat geval zullen verwerkingsverantwoordelijken :

- een hele reeks AVG-verplichtingen, zoals transparantie, naar de betrokken personen toe verzekeren;
- veiligheid van de gegevens waarborgen;
- eventueel een gegevensbeschermingseffectbeoordeling uitvoeren; en
- over een gepaste wettelijke basis tot verwerking dienen te beschikken.

De temperatuur van een natuurlijke persoon is een persoonsgegeven. Meer nog, de temperatuur van een persoon behoort tot een bijzondere categorie van persoonsgegevens. De waarde van lichaamstemperatuur is nl. op zich een persoonsgegeven over gezondheid.

De AVG beschermt persoonsgegevens die geautomatiseerd worden verwerkt of bestemd zijn om in een bestand te worden opgenomen (of daar al in zitten). Gaat het over gezondheidsgegevens, dan is de verwerking zelfs principieel verboden, behoudens uitzonderingen.

Wanneer valt het temperaturen van natuurlijke personen al dan niet onder de AVG?

SITUATIE 1: LOUTER AFLEZEN VAN TEMPERATUUR, ZONDER REGISTRATIE

Indien de gemeten lichaamswarmte enkel rechtstreeks wordt afgelezen en niet in een bestand wordt geregistreerd, dan is er geen sprake van een verwerking van persoonsgegevens waarop de AVG van toepassing is.

Gaat het dus alleen om het louter aflezen van de temperatuur op een klassieke thermometer, zonder de bedoeling om deze meetgegevens nadien (geïndividualiseerd) vast te leggen, dan valt dat aflezen op zichzelf niet onder de toepassing de AVG en dus ook niet onder het toezicht van de GBA, ook al blijven de algemene principes van de bescherming van de persoonlijke levenssfeer wel van toepassing.

Een voorbeeld hiervan is het opnemen van de temperatuur van werknemers met als doel geanonimiseerd te rapporteren (vb. percentage van personen met verhoogde temperatuur, zonder evenwel enige koppeling – ook niet achteraf - mogelijk is met identificeerbare personen).

Uiteraard is het vaak precies de bedoeling om bijkomende stappen te ondernemen ten aanzien van personen die weigeren hun temperatuur te laten meten, of die bij een meting koorts zouden vertonen: deze personen zullen nl. de toegang tot de gebouwen worden ontzegd om verder besmettingsgevaar te vermijden.

Indien daarbij geen bijkomende registratie van identificeerbare personen aan te pas komt, zal er nog steeds geen sprake zijn van een verwerking van persoonsgegevens waarop de AVG van toepassing is.

Een voorbeeld hiervan is de registratie van de temperatuur van bezoekers (van bijvoorbeeld een ziekenhuis, een museum of bibliotheek): de bezoeker zal bij het weigeren van de temperatuuropname of bij verhoogde temperatuurmeting normaliter enkel de toegang tot het gebouw worden ontzegd zonder verdere registratie. In dat geval is er nog steeds geen sprake van een verwerking van persoonsgegevens waarop de AVG van toepassing is.

SITUATIE 2: AFLEZEN VAN TEMPERATUUR MET REGISTRATIE

Indien na het opnemen van de temperatuur verdere stappen evenwel gepaard gaan met een bijkomende registratie (bv. om een weigering van toegang te rechtvaardigen t.o.v. betrokkene, of om deze te documenteren voor andere doelstellingen), zal er daarentegen wel sprake zijn van een verwerking van persoonsgegevens waarop de AVG van toepassing is.

In deze context kunnen we bv. denken aan personeelsleden die hun werkplek niet mogen betreden en leveranciers die hun lading niet mogen afleveren: gezien zij "onverrichter zake" naar huis worden gestuurd zullen onvermijdelijk bijkomende verwerkingen moeten opgezet worden om ten aanzien van hen een dergelijke "lock-out maatregel" (mogelijk zelfs met financiële impact) te rechtvaardigen. M.a.w. voor hen zullen, ook al zou het meetresultaat op zich niet worden vastgelegd, de resultaten van die meting nadien concreet worden gelinkt aan hun "dossier" en/of identiteit en dus als persoonsgegevens worden verwerkt.

Een voorbeeld hiervan is de registratie van de temperatuur in een schoolse context. Ook al wordt de afgelezen temperatuur zelf niet geregistreerd, maar wel een aantekening gemaakt in het leerlingendossier dat iemand afwezig of ziek is, dan gaat het uiteraard wel om een verwerking van (mogelijk zelfs medische) persoonsgegevens, waarop de AVG wel van toepassing is en waarvoor geen grondslag voorhanden is. Dit is onder de huidige wetgeving dus niet toegelaten. In dit geval, net zoals in een arbeidscontext (werkgever-werknemer), kan immers omwille van een gebrek aan gelijkheid tussen de betrokken partijen ook niet worden teruggevallen op de toestemming van de betrokkene.

Voor alle duidelijkheid: indien de gemeten temperatuur zelf van identificeerbare personen in een bestand wordt vastgelegd, dan is er altijd sprake van een (niet-toegelaten) verwerking van persoonsgegevens over gezondheid.

Het verwerken van dergelijke gezondheidsgegevens is principieel verboden, behoudens uitzonderingen (cf. infra).

SITUATIE 3: GEAVANCEERDE ELEKTRONISCHE METING

De AVG is bovendien niet alleen van toepassing bij de vastlegging van persoonsgegevens in een bestand, maar ook als een verwerking op een geavanceerde digitale wijze plaatsvindt, wat het geval is als men automatisch (of vanop afstand) de huidtemperatuur van een persoon meet. In dat geval worden de gegevens immers niet louter afgelezen, maar voorafgaand (elektronisch) verwerkt.

Bij dergelijke geautomatiseerde verwerking moet men immers denken aan alle in artikel 4.2) AVG genoemde verwerkingen die geautomatiseerd (niet handmatig) worden uitgevoerd, waaronder reeds de loutere digitale verzameling zonder verdere opslag of vastlegging.

Onder “verwerken” behoort immers niet alleen het opslaan van gegevens. Alleen al het geavanceerd digitaal temperaturen van personen op zich (d.i. verdergaan dan het loutere aflezen), is een geautomatiseerde verwerking onder de AVG.

Dit houdt dan ook in dat het gebruik van digitale geavanceerde koortsscanners, hittecamera’s of andere geautomatiseerde systemen die de waarde van lichaamswarmte meten op zich een verwerking van persoonsgegevens over gezondheid inhoudt en dus niet toegelaten is.

De vervolgstap na een dergelijke geautomatiseerde temperatuurmeting kan op zijn beurt al dan niet geautomatiseerd verlopen. Er kan sprake zijn van menselijke interventie, waarbij een bewaker die de opname van de temperatuur mee overziet, de persoon die koorts ontwikkelt staande houdt en hem de toegang tot het gebouw ontzegt, maar men heeft ook meer geavanceerde systemen waarbij personen vanop afstand op koortssymptomen worden gescreend en waarbij de toegangspoort tot het gebouw automatisch dicht blijft voor personen die koorts blijken te ontwikkelen.

In dat laatste geval bestaat zelfs het risico dat de betrokkenen niet eens beseffen dat ze eigenlijk op afstand onderworpen zijn geweest aan een heimelijk koortsdetectiesysteem. Dit zou uiteraard bovendien volstrekt onverenigbaar zijn met de transparantievereisten uit de AVG.

De AVG is van toepassing, wat nu?

RECHTSGROND

Indien het temperaturen op zich of eventueel naderhand gepaard gaat met een verwerking van persoonsgegevens, en meer bepaald persoonsgegevens over gezondheid, stelt zich een probleem, want de verwerking van dergelijke gegevens over gezondheid is immers principieel verboden (zie artikel 9, lid 1 AVG). Een verwerkingsverantwoordelijke moet ten aanzien van betrokkenen en de GBA kunnen aantonen dat hij een uitzondering in de zin van artikel 9.2 AVG kan inroepen om niet te zijn onderworpen aan het verwerkingsverbod.

De relevante uitzonderingen in artikel 9.2 AVG betreffen:

> “de betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking van die persoonsgegevens voor een of meer welbepaalde doeleinden, behalve indien in Unierecht of lidstatelijk recht is bepaald dat het in lid 1 genoemde verbod niet door de betrokkene kan worden opgeheven”;
> “de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht, voor zover zulks is toegestaan bij Unierecht of lidstatelijk

recht of bij een collectieve overeenkomst op grond van lidstatelijk recht die passende waarborgen voor de grondrechten en de fundamentele belangen van de betrokkene biedt";
"de verwerking is noodzakelijk om redenen van zwaarwegend algemeen belang, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene";
"de verwerking is noodzakelijk om redenen van algemeen belang op het gebied van de volksgezondheid, zoals bescherming tegen ernstige grensoverschrijdende gevaren voor de gezondheid of het waarborgen van hoge normen inzake kwaliteit en veiligheid van de gezondheidszorg en van geneesmiddelen of medische hulpmiddelen, op grond van Unierecht of lidstatelijk recht waarin passende en specifieke maatregelen zijn opgenomen ter bescherming van de rechten en vrijheden van de betrokkene, met name van het beroepsgeheim."

UITDRUKKELIJKE TOESTEMMING

Er geldt een uitzondering op het algemeen verbod op de verwerking van persoonsgegevens over gezondheid ingeval de betrokkene zijn uitdrukkelijke toestemming geeft.

Eén van de vereisten voor een geldige toestemming is dat die toestemming vrijelijk moet zijn gegeven. Zie ter zake overweging 42 AVG: "Toestemming mag niet worden geacht vrijelijk te zijn verleend indien de betrokkene geen echte of vrije keuze heeft of zijn toestemming niet kan weigeren of intrekken zonder nadelige gevolgen".

Uitdrukkelijke toestemming vragen aan de betrokkene om dergelijke gegevens vast te leggen zal dus problematisch zijn. Toestemming veronderstelt immers dat de betrokkene een keuze heeft en dat hij dus ook kan weigeren in te stemmen met de verwerking.

De toestemming in een arbeidscontext bv. zou precair zijn. Een werknemer kan zich nl. onder druk gezet voelen om toestemming te geven, gezien de afhankelijkheidsrelatie.

Wanneer het weigeren van de toestemming als gevolg heeft dat de toegang tot een gebouw dat men wenste te betreden, wordt geweigerd, kan ook bezwaarlijk van een vrije toestemming worden gesproken.

De aandacht dient er eveneens op gevestigd te worden dat het verkrijgen van een eventuele toestemming een overmatige verwerking nog niet rechtvaardigt. Dit is onder meer het geval wanneer de verwerking niet absoluut noodzakelijk is om het beoogde resultaat te bereiken.

Toestemming zal dus in de meeste omstandigheden geen geschikte rechtsgrond zijn voor het verwerken van de lichaamstemperatuur.

OP GROND VAN HET RECHT VAN DE LIDSTAAT

Het verwerkingsverbod is op grond van artikel 9.2 AVG evenmin van toepassing als de toelating voor verwerken/registratie op grond van het recht van een lidstaat is bepaald, waarbij beoordeeld moet worden of dit evenredig is met het beoogde doel en de privacy is gewaarborgd.

In België bestaat er momenteel geen specifieke wettelijke bepaling die het verwerkingsverbod buiten toepassing laat in de context die voorligt.

Een werkgever bv. heeft weliswaar de algemene verplichting als een goed huisvader te zorgen dat de arbeid wordt verricht in behoorlijke omstandigheden met betrekking tot de veiligheid en de gezondheid van de werknemer (art. 20, 2° Arbeidsovereenkomstenwet van 3 juli 1978, maar deze bepaling is niet voldoende specifiek om in de context die voorligt te kunnen gelden als een passende wettelijke uitzondering op het verwerkingsverbod van artikel 9.1 AVG.

Gelet op de bewoordingen van artikel 9.2.b) AVG is, althans binnen een arbeidscontext, een regeling via een (NAR)-CAO evenmin uitgesloten. Echter, van een dergelijke regeling is er momenteel evenmin sprake in de context die voorligt.

Ook in de schoolcontext heeft de GBA geen weet van een specifieke wettelijke bepaling die het verwerkingsverbod opheft in het kader van systematisch temperaturen bij het betreden van de school.

Gezien er momenteel dus geen solide rechtsgrond voorhanden is om het verwerkingsverbod van artikel 9.1 AVG te doorbreken, roept de GBA de overheid op wetgeving aan te nemen die de bedoelde verwerking van gegevens over gezondheid zou toestaan voor zover de overheid van oordeel zou zijn dat dergelijke verwerkingen mogelijk moeten zijn in het licht van de uitzonderlijke aard van de coronacrisis en zolang die crisis aanhoudt. De vastgestelde wet zal de rechten en vrijheden van de betrokkenen moeten beschermen en in verhouding staan tot het nagestreefde doel. Afwijkingen en beperkingen zullen alleen van toepassing mogen zijn voor zover strikt noodzakelijk.

OVERIGE VERPLICHTINGEN

Indien de AVG van toepassing is, geldt uiteraard voor de verwerkingsverantwoordelijke de verantwoordingsplicht (“accountability”). Hij moet kunnen aantonen dat hij een uitzondering in de zin van artikel 9.2 AVG kan inroepen om niet te zijn onderworpen aan het verwerkingsverbod.

Verder moet de verwerkingsverantwoordelijke technische en organisatorische maatregelen treffen bij het temperaturen van personen. De verplichting van gegevensbescherming door ontwerp vereist dat thermometers moeten gebruikt worden die een minimum aan persoonsgegevens verwerken. Zo dienen er idealiter thermometers gebruikt te worden die geen waardes registreren in een geheugen. Ook is het niet noodzakelijk om hittecamera’s te linken

met een ander IT-systeem, zoals bijvoorbeeld bewakingscamera's of automatische poortjes. De gebruikte toestellen moeten ook accurate resultaten kunnen weergeven en regelmatig gecontroleerd worden met behulp van kalibratie zodat ze geen oneigenlijke resultaten weergeven. De temperatuurwaardes dienen ten slotte ook vergeleken te worden met een vooraf bepaalde drempelwaarde.

De temperatuurmetingen dienen op een transparante wijze plaatstvinden. Zo moet de betrokkene geïnformeerd worden over het doel van de temperatuurmeting. In het geval dat er bij de eerste meting een verhoogde temperatuur is vastgesteld, moet er een procedure voorhanden zijn die bepaalt wat er in deze situatie gebeurt. Zo moet er een tweede meting mogelijk zijn voor de betrokkene om een defect of kalibratieprobleem van het toestel uit te sluiten.

Conclusie

De GBA beschouwt het louter aflezen van de temperatuur niet als een verwerking van persoonsgegevens, voor zover de temperatuur of overige gevolgen (vb. afwezigheid op het werk of op school) niet worden geregistreerd. De AVG is dan niet van toepassing.

Van zodra sprake is van een geheel of gedeeltelijk geautomatiseerde verwerking of opname van gegevens in een bestand, is de AVG wel van toepassing en moet de verwerkingsverantwoordelijke rekening houden met alle basisprincipes van gegevensbeschermingsrecht (vb. legitimiteit, transparantie, minimale gegevensverwerking, gegevensbeveiliging, enz.).

In afwachting van een voldoende duidelijke en specifieke juridische rechtsgrond (vb. door wet of CAO), mogen verwerkingsverantwoordelijken momenteel echter niet:

- personen temperaturen met het oog op het nadien opnemen van het meetresultaat in een bestand;
- personen temperaturen, indien de gevolgen van het meetresultaat voor betrokkene nadien in een bestand worden opgenomen;
- personen temperaturen aan de hand van geavanceerde elektronische meettoestellen zoals koortsscanners, hittecamera's of andere geautomatiseerde systemen die de waarde van lichaamswarmte meten.

Tenslotte wijst de GBA erop dat het meten van koorts als maatregel in de strijd tegen de verspreiding van Covid-19 ten dele ondoelmatig blijft, omdat enerzijds Covid-19 niet steeds met koorts gepaard gaat en anderzijds koorts niet steeds op Covid-19 wijst.

Gezondheidsapps

Allerlei soorten gegevens worden verwerkt in de bestrijding van de COVID-19 epidemie. Ook voor ons zijn volksgezondheid en de bestrijding van de verspreiding uiteraard van het allergrootste belang. We zien echter apps ontstaan die daarbij de bestaande regels niet respecteren en brengen daarom een aantal uitgangspunten in herinnering.

1. Anoniem

Indien er voor het nuttig gebruik van de app door de patiënt geen nood is om persoonsgegevens te verwerken, geschiedt dit niet. In dat geval mogen aan de gebruiker geen rechtstreeks identificerende gegevens (naam en voornaam, mailadres, identificatienummer rijksregister, GSM-nummer, …) worden gevraagd. Er mogen ook geen gegevens worden opgevraagd of gebruikt (vb. identificatie van het toestel of connectie) waarvan de combinatie toelaat de patiënt onrechtstreeks te identificeren. Let wel op: gegevens zijn enkel (voldoende) anoniem, als zij ook in combinatie met andere gegevens (ook van andere partijen) niet meer tot her-identificatie kunnen leiden (vb. IP adressen zijn altijd persoonsgegevens, want met de hulp van een telecomoperator kan men iemand re-identificeren).

2. Zorgrelatie

Indien het gebruik van de app kadert binnen een bestaande zorgrelatie van een patiënt met een zorgverstrekker of een zorginstelling, wordt dat uitdrukkelijk aangegeven en wordt er ook voor gezorgd dat de persoonsgegevens enkel worden verwerkt in het kader van de kwaliteit en de continuïteit door die zorgverlener of door andere zorgverleners die een zorgrelatie hebben met de patiënt. De patiënt wordt dan bij voorkeur door de zorgverlener uitgenodigd om de app te gebruiken.

3. Andere gevallen

In de situaties waar 1. of 2. niet van toepassing zijn, dient een app, die persoonsgegevens verwerkt, op het allereerste scherm, en voordat de gebruiker enig persoonsgegeven ingeeft of gegevens van hem worden gebruikt, de informatie te verstrekken die wordt vereist door de AVG (verwerkingsverantwoordelijke, precies doel van de verwerking, gebruik van cookies…). Rechtstreeks identificerende persoonsgegevens (naam en voornaam, mailadres, identificatienummer rijksregister, GSM-nummer, …) worden niet opgevraagd bij het begin van het gebruik van de app. Tijdens het gebruik van de app worden enkel persoonsgegevens gebruikt voor de goede werking van de app binnen het kader van het vermelde doeleinde en onder de verantwoordelijkheid van de vermelde verwerkingsverantwoordelijke. Op het einde van het gebruik van de app kan aan de patiënt worden gevraagd of hij zijn persoonsgegevens wil laten doorgeven in het kader van een bestaande zorgrelatie (vb. resultaat van zijn zelfevaluatie

doorgeven aan de huisdokter), of om een nieuwe zorgrelatie aan te maken. Zo ja, dan kunnen de nodige bijkomende persoonsgegevens worden opgevraagd en doorgegeven, zoniet worden alle persoonsgegevens gewist en niet verder gebruikt.

Opsporingsapplicaties en COVID-19 databanken: voor de GBA moeten de voorontwerpen van koninklijke besluit worden herzien

De Gegevensbeschermingsautoriteit (GBA) is met spoed geraadpleegd om advies uit te brengen over twee voorontwerpen van koninklijke besluit betreffende respectievelijk het gebruik van opsporingsapplicaties en het oprichten van een databank "om de verspreiding van het coronavirus te voorkomen". De bescherming van persoonsgegevens vormt geen belemmering voor het gebruik van technologische instrumenten in de strijd tegen de COVID-19-epidemie, zolang zij bepaalde fundamentele beginselen in acht nemen. De normatieve teksten die het gebruik van deze instrumenten voorzien en regelen, moeten nauwkeurig en volledig zijn om een optimale transparantie voor de burger te garanderen en de noodzaak om beroep te doen op een opsporingsapplicatie, moet worden aangetoond, aldus de GBA.

Bijkomende garanties voor de burger

Dit onderwerp heeft al veel inkt doen vloeien: in de strijd tegen de verspreiding van het coronavirus is het de bedoeling om de contacten op te sporen die een positief getest persoon kan hebben besmet. Deze opsporing zou kunnen gebeuren door te trachten de personen te onthouden wiens pad men heeft gekruist en bijkomend, via een applicatie (die zou werken op basis van digitale sleutels die de betrokken personen niet rechtstreeks identificeren).

Het Kenniscentrum van de GBA, dat bevoegd is om adviezen te formuleren over normatieve ontwerpen, is geraadpleegd over twee voorontwerpen van koninklijke besluit, die een kader bieden voor het gebruik van digitale contactopsporingsapplicaties en voor de oprichting van een databank door Sciensano. De adviezen over deze ontwerpen bevatten talrijke overwegingen die kunnen worden samengevat in twee essentiële punten:

- De noodzaak en de proportionaliteit van opsporingsapplicaties en het opzetten van een databank bij Sciensano, moet worden aangetoond :
  - Ingrijpen in het privéleven van burgers, zoals mogelijk gemaakt door deze koninklijke besluiten, is alleen toegestaan als dit noodzakelijk is en in verhouding

staat tot de verwezenlijking van het doeleinde van algemeen belang dat erin bestaat de verspreiding van het virus tegen te gaan.
De invoering van een opsporingssysteem door middel van applicaties is alleen toegestaan als dit het minst ingrijpende middel is om het nagestreefde doel te bereiken en als er een juist evenwicht is tussen de betrokken belangen (proportionaliteit).

De ontwerpen moeten de burgers extra garanties bieden :

De teksten moeten verder worden verduidelijkt om te vermijden dat het zou mislopen. Het besluit betreffende de oprichting van een databank door Sciensano moet duidelijker zijn wat betreft de oorsprong van de verzamelde gegevens, de derden aan wie deze medische gegevens mogen worden doorgegeven en het gebruik dat zij ervan mogen maken.
In de teksten moet ook worden bepaald dat er geen kruising mogelijk zal zijn tussen de verschillende databanken die in het kader van de bestrijding van de epidemie zijn opgezet (of met een andere databank), en ook dat de verzamelde gegevens niet voor andere doeleinden mogen worden hergebruikt.

De minimale vereisten voor een opsporingsapplicatie

Naast haar opmerkingen over de voorontwerpen herinnert de GBA eraan dat elke opsporingsapplicatie moet voldoen aan de regels en specificaties die zijn vastgesteld door het EDPB (Europees Comité voor gegevensbescherming waarin de GBA een actieve rol speelt), dat hierover onlangs richtsnoeren en een "toolbox" heeft gepubliceerd.

Zo moet er bijvoorbeeld voor worden gezorgd dat het downloaden en gebruiken van een opsporingsapplicatie echt vrijwillig is en dat geen enkele burger die weigert om er gebruik van te maken, nadeel kan ondervinden (zoals het feit dat hem de toegang tot een goed of dienst wordt ontzegd).

De broncode van elke applicatie zal ook op voorhand moeten worden gepubliceerd, zodat de deskundigen een redelijke termijn krijgen om de werking ervan te controleren. Elke applicatie moet ook worden onderworpen aan een effectbeoordeling voordat deze wordt gelanceerd en, indien uit deze beoordeling blijkt dat er verhoogde risico's bestaan, moet deze voor advies worden voorgelegd aan het Algemeen Secretariaat van de GBA.

De volksgezondheid is essentieel voor de GBA

Voor de GBA is de volksgezondheid van het grootste belang en het behoud ervan is niet onverenigbaar met het recht op privacy.

David Stevens, Voorzitter van de GBA herhaalt: "Opsporing om de volksgezondheid te beschermen ligt ons zeer nauw aan het hart. Hier raken we aan twee belangrijke prioriteiten van de GBA: gevoelige (medische) gegevens enerzijds en de verwerking van gegevens door de overheid anderzijds."

De GBA heeft sinds het begin van de coronacrisis hard gewerkt om oplossingen te helpen vinden die doeltreffend zijn tegen COVID-19, maar die tegelijk ook de persoonsgegevens van de burgers met respect behandelen. Naast de deelname aan de Europese reflectie over het onderwerp en het binnen zeer korte termijnen verstrekken van adviezen over ontwerpnormen of effectbeoordelingen, heeft de GBA op haar website ook een dossier gepubliceerd dat volledig gewijd is aan het coronavirus.

Alexandra Jaspar, Directeur van het Kenniscentrum van de GBA, besluit: "De regels inzake gegevensbescherming vormen in principe geen belemmering voor de totstandkoming van een kader dat het gebruik van een opsporingsapplicatie mogelijk maakt. Dit kader moet echter wel een aantal bakens in acht nemen die zijn voorzien in de Algemene Verordening Gegevensbescherming en die nader zijn toegelicht door de verschillende Europese autoriteiten die deel uitmaken van het Europees Comité voor gegevensbescherming."

Mag ik wel de persoonsgegevens (zoals telefoonnummer, naam en voornaam) opgeven van de personen met wie ik contacten had om te antwoorden op de vragen van een contactonderzoeker? Overtreed ik dan niet de AVG?

Laatste update: 04/02/2021

Ja, u mag dit. U kan de persoonsgegevens van contactpersonen met de contactonderzoeker delen zonder de AVG te schenden omdat de overheid hiervoor een bijzonder wettelijke regeling heeft aangenomen.

Een besmette persoon geeft de persoonsgegevens van zijn contacten vrij aan een contactonderzoeker op grond van een wettelijke toelating, meer bepaald het samenwerkingsakkoord van 25 augustus 2020. Bijgevolg hebt u niet de toestemming nodig van uw contactpersonen om deze informatie mee te delen aan de contactonderzoeker.

Het is de bedoeling dat de contactonderzoeker op grond van de meegedeelde persoonsgegevens in staat is om de personen waarmee u in contact kwam, en die daardoor mogelijk ook besmet werden, op te sporen en hun de nodige aanbevelingen mee te geven (thuis blijven, thuis werken, enz.). Dit is nodig om te vermijden dat die personen op hun beurt nog andere mensen in hun omgeving ziek zouden maken.

Voor meer informatie over het contactonderzoek verwijzen wij u door naar de webpagina van de FOD Volksgezondheid.

Kan de informatie die de overheid verzamelt in het kader van contactonderzoek later gebruikt worden om mij te sanctioneren indien blijkt dat ik de regels niet naleefde?

Laatste update: 04/02/2021

Neen, de overheid mag dit niet.

De overheid mag deze informatie niet gebruiken om u later te sanctioneren. De informatie die contactonderzoekers verzamelen wordt opgeslagen in een federale databank die werd opgericht door het samenwerkingsakkoord van 25 augustus 2020.

Het samenwerkingsakkoord somt alle doeleinden op waarvoor de persoonsgegevens in deze federale databank mogen gebruikt worden, met name: het opsporen en contacteren van personen in de strijd tegen Covid-19, het ondersteunen van beleidsondersteunend, wetenschappelijk onderzoek en het inlichten van de gezondheidsinspectiediensten van de Gewesten. De persoonsgegevens in de federale databank mogen uitsluitend worden gebruikt voor deze doeleinden.

De doorgifte van de persoonsgegevens aan de politie of gerechtelijke instanties om niet-naleving van bepaalde coronamaatregelen te bestraffen is onverenigbaar met deze oorspronkelijke doeleinden en zou een manifeste inbreuk inhouden op het principe van doelbinding. De informatie die een besmette persoon geeft aan de contactonderzoeker mag dus niet gebruikt worden om te controleren of de betrokkene de door de overheid opgelegde coronamaatregelen naleefde.

Mag ik weigeren om personen met wie ik in contact kwam door te geven aan de contactonderzoeker?

Ja, u mag weigeren.

U bent immers niet verplicht om te antwoorden op alle vragen van de contact-onderzoeker. Hoewel er geen harde wettelijke verplichting is om de contactgegevens van uw contacten door te geven, rekent de overheid op de burgerzin van elke besmette persoon om zo transparant mogelijk te zijn over zijn contacten en op die manier verdere besmettingen te beperken.

Voor meer informatie over het contactonderzoek verwijzen wij u door naar de webpagina van de FOD Volksgezondheid.

Moet de contactonderzoeker niet meedelen van wie hij mijn contactgegevens heeft gekregen?

Laatste update: 04/02/2021

Neen, de contactonderzoeker moet u deze informatie niet meedelen omdat de overheid hiervoor een bijzonder wettelijke regeling heeft aangenomen.

In dit geval heeft de verwerkingsverantwoordelijke (hier: het contactcentrum) uw persoonsgegevens op onrechtstreekse wijze verkregen bij een derde, namelijk de besmette persoon. Normaal schrijft artikel 14 AVG voor dat de verkrijgende verwerkingsverantwoordelijke de betrokkenen (hier: u) moet inlichten over de bron van de persoonsgegevens. Op die manier zou u kunnen weten welke besmette persoon uw persoonsgegevens doorgaf.

Deze informatieplicht hier echter niet van toepassing omdat artikel 14.5.c) AVG een uitzondering bevat wanneer het verkrijgen of verstrekken van de gegevens uitdrukkelijk is voorgeschreven door een wettelijke regeling die voorziet in passende maatregelen om de gerechtvaardigde belangen van de betrokkene te beschermen. In België is deze regeling het samenwerkingsakkoord van 25 augustus 2020.

Voor meer informatie over het contactonderzoek verwijzen wij u door naar de webpagina van de FOD Volksgezondheid.

Schend ik mijn beroepsgeheim wanneer ik de contactgegevens doorgeef van personen met wie ik in contact kwam in het kader van mijn beroep (bv. Als maatschappelijk werker sociale dienst, actief in de thuiszorg, arbeidstrajectbegeleider, arts,…)?

Laatste update: 04/02/2021

Neen, u schendt uw beroepsgeheim niet. Ook indien de besmette persoon drager is van het beroepsgeheim, zal hem of haar, zoals elke andere besmette burger, gevraagd worden de personen waarmee hij of zij recent in contact kwam mee te delen aan de contactonderzoeker.

De Autoriteit wijst op het samenwerkingsakkoord van 25 augustus 2020. Dit samenwerkingsakkoord voorziet een wettelijke uitzondering op de geheimhoudingsplicht voor

gezondheidszorgbeoefenaars in het kader van contactopsporing. Verder zijn volgens dit samenwerkingsakkoord ook andere personen die drager zijn van een geheimhoudingsplicht hiervan ontheven en mogen zij contactgegevens doorgeven in het kader van contactopsporing indien ze zelf een positieve Covid-19-test hebben afgelegd of indien de arts een ernstig vermoeden heeft dat ze besmet zijn met het Covid-19.

Naar analogie is de Autoriteit van oordeel dat ook andere beroepsgroepen die niet expliciet vermeld worden in het samenwerkingsakkoord met een beroepsgeheim medewerking mogen verlenen aan de contactopsporing zonder hun beroepsgeheim te schenden.

Bovendien kan de contactonderzoeker niet weten welke informatie de besmette persoon meedeelt als geheimplichtige (bijv. namen van patiënten en cliënten die onder het beroepsgeheim vallen) dan wel als burger (bijv. namen van vrienden, collega's, kennissen, familieleden, etc.…).

Verzamelen van contactgegevens in de horeca in het kader van de strijd tegen COVID-19

Sinds zaterdag 25 juli zijn horeca-uitbaters verplicht de contactgegevens van hun klanten te verzamelen in de strijd tegen de verspreiding van Covid-19. Deze verplichting werd nadien uitgebreid tot andere gelegenheden of evenementen, zoals gemeenschappelijke sportlessen, casino's, enz. Ze werd opgelegd door de ministeriële besluiten van 30 juni 2020 en 28 juli 2020(hierna "de besluiten").

De GBA ziet tal van initiatieven tot ontwikkeling komen bij de uitvoering van deze besluiten die, omdat ze geen nauwkeurige informatie verstrekken, meer bepaald over de specifieke rol van de verschillende actoren die betrokken zijn bij het verzamelen van de gegevens of over de middelen die daarbij ingezet moeten worden, hierdoor heel wat vragen onbeantwoord laten.

Tegen die achtergrond wil de GBA voor de zaakvoerders de essentiële punten verduidelijken die in acht genomen moeten worden bij het invoeren van systemen, manuele of elektronische, die toelaten de gegevens te verzamelen zoals bedoeld in deze besluiten.

In de praktijk: toepassen van de beginselen van de AVG

De grondbeginselen van de Algemene Verordening Gegevensbescherming (of AVG) zijn steeds van toepassing en moeten dus nageleefd worden bij de verplichte verzameling van contactgegevens van de klanten van gelegenheden zoals bedoeld in de ministeriële besluiten. Hier volgen de voornaamste:

Minimale gegevensverwerking

De persoonsgegevens die verzameld worden door de zaakvoerders zoals bedoeld in de besluiten, moeten beperkt blijven tot wat noodzakelijk is met betrekking tot de doeleinden waarvoor ze verwerkt worden.

De besluiten bepalen in de Franse versie dat de verzamelde gegevens “zich mogen beperken tot” een telefoonnummer of e-mailadres. In het Frans verschilt de formulering van de Nederlandse tekst, die veel preciezer is en duidelijk de gegevens beperkt die verzameld mogen worden.

De zaakvoerders mogen dus enkel de gegevens verzamelen die nodig zijn om te voldoen aan hun wettelijke verplichting, namelijk:

> het e-mailadres of het telefoonnummer (waarbij de uitbater dus niet mag eisen dat deze twee gegevens tegelijk verstrekt worden);
> van één persoon per tafel/reservering.

Naast deze persoonsgegevens zijn we van mening dat de datum (en eventueel het tijdstip) van het bezoek/de aankomst van de klant in de gelegenheid bewaard moet(en) worden, aangezien deze gegevens noodzakelijk zijn voor de verwerking, gelet op het doeleinde en ook om het startpunt van de bewaartermijn van de gegevens te bepalen.

Hoewel er geen melding van wordt gemaakt in de besluiten, zijn we van mening dat de naam en voornaam van de betrokken persoon op vrijwillige basis ingezameld kunnen worden (ze staan trouwens vermeld op het formulierdat aangeboden wordt op de website van de FOD Economie). Deze voorziet tevens de optionele vermelding van het tafelnummer en de duur van het verblijf wanneer dit gerechtvaardigd is.

Het is essentieel dat het optionele karakter van het verstrekken van deze gegevens duidelijk vermeld wordt op het inzamelmedium dat aan de klanten voorgelegd wordt.

In geval geautomatiseerde systemen gebruikt worden, zoals bijvoorbeeld een online formulier of een app, is het belangrijk dat deze systemen zo zijn ingesteld dat ze enkel de hierboven vermelde gegevens inzamelen en geen andere.

Proportionaliteit

De verwerking van persoonsgegevens moet steeds passend, relevant en in verhouding zijn ten opzichte van het beoogde doel.

Aangezien de besluiten niet voorzien welk(e) systeem(-emen) (manuele of elektronische) gebruikt mag/mogen of moet(en) worden om de contactgegevens van de klanten te verzamelen, hebben de horeca-uitbaters een zekere mate van vrijheid wat dat betreft. Het dient echter

opgemerkt dat de FOD Economie op haar website een papieren formulier heeft aangeboden die in een enveloppe bewaard moet worden.

Doelbinding

Persoonsgegevens mogen in principe enkel verwerkt worden voor het doel waarvoor ze verzameld werden. In dit geval voorzien de besluiten dat de contactgegevens enkel verwerkt mogen worden ten behoeve van “de strijd tegen Covid-19”, met uitsluiting van ieder ander doel.

De zaakvoerders die verplicht zijn om de contactgegevens van hun klanten te verzamelen, mogen de gegevens die verkregen werden om te voldoen aan deze wettelijke verplichting dus niet gebruiken voor een ander doel. Zo mogen ze bijvoorbeeld geen bericht sturen naar het door de klant opgegeven e-mailadres om te vragen of de maaltijd hem is bevallen, of hij wenst terug te keren en of hij zich wil abonneren op de nieuwsbrief. Deze gegevens mogen in geen geval toegevoegd worden aan de databank van klanten en potentiële klanten van de gelegenheid en mogen ook niet meegedeeld worden aan andere ondernemingen.

Bewaartermijn

De AVG bepaalt dat persoonsgegevens slechts bewaard mogen worden voor de duur die nodig is om de doeleinden te vervullen waarvoor ze verzameld werden.

De besluiten voorzien erin dat de gegevens die verzameld worden door de verantwoordelijken van de gelegenheden bewaard worden gedurende een periode van 14 dagen. Bijgevolg moeten de horeca-uitbaters deze gegevens definitief verwijderen/vernietigen na afloop van deze termijn. Als er een besmetting wordt vastgesteld vóór het einde van de termijn van 14 dagen, worden de gegevens meegedeeld aan de bevoegde autoriteiten.

De verantwoordelijke zaakvoerders moeten dus een systeem invoeren waarmee de gegevens effectief vernietigd worden op het einde van de voorziene termijn, en dit ongeacht de wijze waarop ze deze gegevens verzameld hebben (papiervorm, elektronisch formulier enz.). Een inzameling “op papier/in handgeschreven vorm” van de gegevens gegroepeerd volgens datum van inzameling, zal de vernietiging ervan vergemakkelijken. In een digitale omgeving, in geval de gegevens via een derde app verzameld worden, riskeert de bar/restaurantuitbater de controle over de correcte vernietiging van de gegevens te verliezen. Die controle krijgt hij terug als hij de gegevens lokaal, op zijn eigen computersysteem, verwerkt.

Veiligheid en vertrouwelijkheid van de gegevens

De personen die instaan voor de gegevensverwerking moeten alle passende technische en organisatorische maatregelen nemen om de veiligheid en vertrouwelijkheid van de gegevens te

garanderen, meer bepaald om ongeoorloofde toegang tot deze gegevens te vermijden. Concreet moeten deze maatregelen garanderen dat de gegevens enkel toegankelijk zullen zijn voor bevoegde personen (vertrouwelijkheid), dat ze beschikbaar zullen zijn wanneer men ze nodig heeft in het kader van opsporing (beschikbaarheid) en dat ze niet gewijzigd werden na de verzameling ervan (integriteit). De besluiten voorzien wat dat betreft niet in concrete maatregelen.

Om de vertrouwelijkheid van de gegevens in het kader van een "papieren" gegevensverzamelingssysteem te verzekeren, lijken aangewezen maatregelen bijvoorbeeld:

> het papieren formulier niet in het zicht van iedereen laten, bijvoorbeeld: door het uit te hangen op het mededelingenbord van een sportclub of door het neer te leggen op het bureau van het secretariaat met de verplichting voor elk van de leden om na elkaar hun gegevens te komen opschrijven, waardoor de gegevens dus zichtbaar zijn voor alle leden. Als de uitbater met één formulier wil werken waarop de gegevens van zijn verschillende klanten staan, moet hij dit zelf invullen (op basis van de gegevens die de klanten mondeling verstrekken). Als de gegevens door de klanten zelf ingevuld moeten worden, moeten de klanten in de praktijk elk een document krijgen om in te vullen.
> de formulieren opbergen in een afgesloten kast waartoe een specifieke persoon toegang heeft. Dit houdt in dat er ook een vervanger moet voorzien worden in geval deze persoon afwezig is. Een andere oplossing is om ze in verzegelde enveloppen te stoppen.

Bij gebruik van een computersysteem kan de toegang tot de databank bijvoorbeeld beschermd worden met een sterk paswoord, een versleutelingssysteem voor de gegevens enz.

Transparantiebeginsel

De betrokkenen moeten duidelijke en volledige informatie krijgen over de manier waarop hun gegevens verwerkt zullen worden. Er zijn bepaalde uitzonderingen.

De Autoriteit is van mening dat de informatieclausule die vermeld staat op het formulier dat aangeboden wordt op de website van de FOD Economie, als basis kan dienen voor het verstrekken van de nodige informatie aan de klant op voorwaarde dat ze aangevuld en verbeterd wordt, meer bepaald door duidelijk aan te geven wie de gegevens verwerkt en aan welke bevoegde autoriteiten de gegevens meegedeeld zullen worden ingeval een besmetting met Covid-19 zou vastgesteld worden.

Nee. De verwerkingsverantwoordelijke van de persoonsgegevens is gebonden aan een vertrouwelijkheidsplicht. Aldus moet hij de persoonsgegevens die hij verwerkt, beschermen tegen ongeoorloofde toegang. Door een lijst van de klanten en hun contactgegevens uit te hangen

aan de deur of aan de balie van een gelegenheid kan iedereen de gegevens inkijken of zelfs kopiëren of nadien gebruiken. Dit is in strijd met de AVG.

Moet ik het standaardformulier van de FOD Economie gebruiken?

Nee. De besluiten bepalen niet welk(e) systeem(-emen) (manuele of elektronische) gebruikt mag/mogen of moet(en) worden om de contactgegevens van de klanten te verzamelen. De horeca-uitbaters hebben een zekere mate van vrijheid wat dat betreft.

In alle gevallen wordt het standaardformulier door de FOD enkel aangeboden als voorbeeld en moet het eventueel aangepast worden in functie van de specifieke situatie.

Mag ik de contactgegevens verzamelen met behulp van elektronische systemen, bijvoorbeeld een app ?

Ja. De besluiten voorzien niet welk(e) systeem(-emen) (manuele of elektronische) gebruikt mag/mogen of moet(en) worden om de contactgegevens van de klanten te verzamelen. De horeca-uitbaters hebben een zekere mate van vrijheid wat dat betreft.

Ongeacht het systeem dat gebruikt wordt, geldt dat, om wettelijk te zijn, de invoering en werking ervan in overeenstemming moeten zijn met de beginselen van de AVG. Elektronische systemen kunnen bijkomende verplichtingen met zich meebrengen voor de zaakvoerder die verantwoordelijk is voor de verwerking van de contactgegevens. Bij registratie via een app online moet men er bijvoorbeeld voor zorgen dat de regels betreffende de verzameling van gegevens via cookies nageleefd worden en dat er geen bijkomende persoonsgegevens over de gebruiker verzameld worden. De zaakvoerder moet er ook op toezien dat de leverancier van de app de gegevens niet verwerkt voor zijn eigen doeleinden of dat de gegevens werkelijk vernietigd worden na 14 dagen enz.

Mag ik de contactgegevens verzamelen met behulp van de eID?

De besluiten voorzien geen specifiek systeem voor het verzamelen van de contactgegevens. Een verzamelsysteem via eID is dus niet nadrukkelijk verboden. Het is echter niet mogelijk om het lezen van de eID te verplichten om de contactgegevens te verzamelen. De klant moet een alternatief systeem geboden worden.

Zelfs indien de zaakvoerder dit alternatief voorziet, moeten andere beperkingen in verband met de beginselen van de AVG in aanmerking worden genomen.

De verwerkingsverantwoordelijke die de eID wil lezen om de contactgegevens te verzamelen, moet dus een andere wettelijke basis hebben om zijn verwerking te kunnen doen, zoals toestemming. Om geldig te zijn, moet deze voldoen aan alle voorwaarden van de AVG, meer bepaald moet ze specifiek zijn en geïnformeerd en vrij gegeven zijn.

De identiteitskaarten bevatten tal van gegevens die niet verzameld mogen worden in het kader van de besluiten die voorzien in de verzameling van contactgegevens (zoals bijvoorbeeld het fysieke adres). De uitbater moet zich er dus van vergewissen dat vanuit technisch oogpunt enkel de strikt noodzakelijke gegevens op de identiteitskaart gelezen worden. De enige gegevens die in dit verband als noodzakelijk kunnen worden beschouwd zijn de naam en voornaam. Nochtans voorzien de besluiten niet in de verplichting om ze te verzamelen, waardoor het vrijblijvende karakter van de verzameling van deze gegevens benadrukt moet worden. We merken ook op dat noch het telefoonnummer, noch het e-mailadres, die essentiële gegevens zijn voor het doel dat hier beoogd wordt, op de eID staan. Dit doet vragen rijzen over de noodzaak en doeltreffendheid van dit middel aangezien de essentiële contactgegevens, de enige waarin de besluiten voorzien, niet op de identiteitskaart staan en afzonderlijk genoteerd moeten worden.

Voor meer informatie over het lezen van de eID, raadpleeg ons themadossier.

Mogen de verzamelde contactgegevens gebruikt worden voor een ander doel dan contactopsporing in het kader van de strijd tegen Covid-19?

De ministeriële besluiten van 30 juni en 28 juli 2020 bepalen dat deze gegevens “mogen enkel worden gebruikt voor de doeleinden van de strijd tegen COVID-19”, wat laat doorschemeren dat ze door bepaalde autoriteiten hergebruikt zouden mogen worden voor andere doeleinden dan contactopsporing; deze doeleinden zijn jammer genoeg niet gespecificeerd in de besluiten.

De zaakvoerders die verplicht zijn om de contactgegevens van hun klanten te verzamelen, mogen de gegevens die verkregen werden om te voldoen aan deze wettelijke verplichting niet gebruiken voor een ander doel. Zo mogen ze bijvoorbeeld geen bericht sturen naar het e-mailadres dat de klant heeft opgegeven met het oog op de verplichte verzameling van zijn contactgegevens in het kader van de strijd tegen Covid-19 om te vragen of de maaltijd hem is bevallen, of hij wenst terug te keren en of hij zich wil abonneren op de nieuwsbrief. Deze gegevens mogen in geen geval toegevoegd worden aan de databank van klanten en potentiële klanten van de gelegenheid en ook niet meegedeeld mogen worden aan andere ondernemingen.

Op de vraag of deze gegevens doorgegeven zouden mogen worden aan autoriteiten die de bevoegdheid hebben om onderzoek te verrichten, waaronder de verplichte verstrekking van documenten en informatie (bijvoorbeeld in het kader van strafonderzoeken naar aanleiding van

feiten die zich hebben voorgedaan in de gelegenheden), lijkt het antwoord ons positief voor zover deze bevoegdheden zijn ingesteld door hogere normen dan voornoemde besluiten (die erin voorzien dat deze gegevens enkel gebruikt mogen worden door de strijd tegen COVID-19).

Moet ik als zaakvoerder van een gelegenheid die onderworpen is aan de verplichting om contactgegevens te verzamelen, controleren of de door de klant verstrekte gegevens correct zijn?

Nee. De AVG voorziet normaal dat de verwerkte gegevens inderdaad correct moeten zijn, doch de besluiten vermelden niet of (en, zo ja, hoe) de horeca-uitbaters zich moeten vergewissen van de juistheid van de gegevens die door hun klanten verstrekt worden. Men kan er dus van uitgaan dat de controle op de juistheid van de door de klanten verstrekte gegevens in dit geval niet verwacht wordt (en dus niet toegelaten is).

Kan de provinciegouverneur de registratieplicht in de horeca uitbreiden?

Ja, dit kan.

Het ministerieel besluit van 30 juni 2020 bepaalt dat horeca-uitbaters de contactgegevens van één klant per tafel, die zich kunnen beperken tot een telefoonnummer of een e-mailadres, moeten registreren en bewaren gedurende 14 kalenderdagen om later contactonderzoek te vergemakkelijken. Artikel 23 van ditzelfde besluit bepaalt dat de burgemeesters in overleg met de gouverneur en de bevoegde overheden aanvullende maatregelen kunnen nemen ten opzichte van deze voorzien in het ministerieel besluit. De aanvullende maatregelen kunnen een bijkomende verwerking van persoonsgegevens invoeren indien dit reglementair omkaderd en transparant is en de verwerking toereikend is, ter zake dienend en beperkt tot wat noodzakelijk is voor de nagestreefde doeleinden.

Welke persoonsgegevens mag ik als uitbater van een fitnescentrum, horecazaak, zwembad of wellnesscentrum doorgeven aan de bevoegde overheden voor het contactonderzoek?

Artikel 6bis van het ministerieel besluit van 30 juni 2020 legt de verplichting op om de contactgegevens van één bezoeker per huishouden, met name een telefoonnummer of een

e-mailadres, te registreren bij aankomst. Voor de bezoekers die dit weigeren moet u als uitbater de toegang tot uw zaak weigeren.

Naast deze persoonsgegevens mag u het tijdstip van het bezoek noteren omdat dit nodig is voor het doeleinde van het contactonderzoek en het bepalen van de bewaartermijn. Tot slot mag u eveneens de naam en voornaam van de persoon inzamelen zoals vermeld op het formulier van de FOD Economie.

Het ministerieel besluit bepaalt uitdrukkelijk dat u deze persoonsgegevens na 14 kalenderdagen moet vernietigen en dat u ze uitsluitend mag gebruiken voor de strijd tegen COVID-19. U mag de persoons-gegevens (telefoonnummer of e-mailadres) voor geen enkel ander doeleinde gebruiken.

Dit betekent dat wanneer de bevoegde overheidsdiensten (zoals Sciensano, de regionale contactcentra, gezondheidsinspectiediensten en mobiele teams) deze informatie opvragen, u als uitbater verplicht bent om het geregistreerde telefoonnummer of e-mailadres, naam, voornaam en tijdstip van bezoek mee te delen.

Op grond van artikel 5.1 c AVG moeten persoonsgegevens die u doorgeeft beperkt zijn tot wat noodzakelijk is voor het nagestreefde doeleinde. Concreet betekent dit dat u naast het geregistreerde telefoonnummer of e-mailadres, naam, voornaam en tijdstip van bezoek geen andere persoonsgegevens mag meedelen.

Indien de bevoegde overheidsdienst bijkomende persoonsgegevens vraagt, stelt u als uitbater eerst de vraag op basis van welke wettelijke (lokale) maatregel deze opvraging mogelijk is, alvorens dit verzoek in te willigen. Op die manier kan u de rechtmatigheid en proportionaliteit van het verzoek beoordelen.

Verwerking van persoonsgegevens i.v.m. vaccinatie in het kader van de strijd tegen COVID-19

Naar aanleiding van actuele gebeurtenissen omtrent de vaccinatiestrategie tegen Covid-19 ontving de Gegevensbeschermingsautoriteit (“GBA”) een aantal terugkerende vragen over de gevolgen van deze strategie met betrekking tot de verwerking van persoonsgegevens. De huidige strategie bepaalt dat de vaccinatie tegen Covid-19 op vrijwillige basis gebeurt waardoor personen vrij zijn om te kiezen of ze zich laten vaccineren of niet. De GBA lijst op deze pagina de meest gestelde vragen op en wijst op het belang van de bescherming van persoonsgegevens in deze nieuwe fase van de pandemie. De onderstaande antwoorden zijn onderhevig aan eventueel

wettelijke ontwikkelingen over de vaccinatiestrategie en zullen dan ook aangepast worden indien nodig.

De GBA vestigt de aandacht op de regels met betrekking tot de verwerking van gezondheidsgegevens. Informatie over de vaccinatiestatus van een persoon zijn persoonsgegevens onder de Algemene Verordening Gegevensbescherming ("AVG") en meer bepaald gezondheidsgegevens die een ruimer regime van bescherming genieten onder de AVG. Het opvragen en registreren van deze vaccinatiestatus is dan ook een verwerking van gezondheidsgegevens waarop de AVG van toepassing is. Het opvragen van de vaccinatiestatus zal in beginsel verboden zijn, tenzij de verwerkingsverantwoordelijke zich op een uitzondering van artikel 9.2 AVG kan beroepen. Hieronder bespreken we de meest relevante uitzonderingen.

Uitdrukkelijke toestemming

Artikel 9.2.a) AVG stelt dat u gezondheidsgegevens kan verwerken met de uitdrukkelijke en vrije toestemming van de betrokkene. Dit wil zeggen dat de betrokkene een echte, vrije keuze heeft tot zijn toestemming en dat er geen nadelige gevolgen verbonden kunnen worden aan het weigeren of intrekken van de toestemming. Indien de toegang tot een bepaalde plaats afhankelijk wordt gesteld van een vaccinatiebewijs tegen Covid-19, is dit in strijd met het 'vrije' karakter van de toestemming. Bijgevolg is de toestemming voor het verwerken van de vaccinatiestatus van een betrokkene niet vrij als de toegang tot de plaats geweigerd wordt aan personen die zich bewust niet hebben laten vaccineren, de kans nog niet hebben gekregen om zich te laten vaccineren tegen Covid-19 of geen vaccinatiebewijs kunnen voorleggen.

Toestemming zal dus in de meeste omstandigheden geen geschikte rechtsgrond zijn voor het verwerken van de vaccinatiestatus van een persoon.

Op grond van het recht van de lidstaat

Het verbod op het opvragen van de vaccinatiestatus van personen kan ook opgeheven worden op basis van het recht van een lidstaat. Belangrijk hierbij te vermelden is dat een dergelijke maatregel evenredig moet zijn met het beoogde doel en de wezenlijke inhoud van het recht op bescherming van persoonsgegevens moet eerbiedigen. Bovendien moeten er passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkene.

In het geval van een arbeidsrechtelijke relatie kan dit recht van de lidstaat ook vastgelegd zijn in een collectieve arbeidsovereenkomst indien deze passende waarborgen biedt voor de grondrechten en de fundamentele belangen van de betrokkenen. Belangrijk om op te merken is

dat in een arbeidsrelatie deze uitzondering vereist dat de bepaling voldoende specifiek moet zijn in de context die voorligt om te kunnen gelden als passende wettelijke uitzondering op het verwerkingsverbod van artikel 9.1 AVG.

Het is ook mogelijk om de verwerking van gezondheidsgegevens toe te staan op basis van het recht van een lidstaat om een zwaarwegend algemeen belang of de volksgezondheid te beschermen. Dergelijke wetgeving moet evenredig zijn met het nagestreefde doel, het recht op gegevensbescherming van de betrokkenen eerbiedigen en gepaard gaan met specifieke maatregelen om de grondrechten van de betrokkene te beschermen. Een vage of te algemene wetsbepaling is dus niet voldoende.

De GBA heeft op dit ogenblik nog geen kennis genomen van enige wetgeving of CAO die het mogelijk maakt om met het oog op de bescherming tegen de verdere verspreiding van het Covid-19 virus de vaccinatiestatus van een persoon op te vragen en bijgevolg deze gezondheidsgegevens te verwerken.

Kunnen een vliegmaatschappij, restaurant, winkel of openbare dienstverlener bezoekers of klanten om een vaccinatiebewijs vragen?

Nee, de vaccinatiestatus van een persoon is een gezondheidsgegeven. De verwerking van gezondheidsgegevens is krachtens artikel 9 AVG verboden tenzij een wet hierop een uitzondering maakt of de betrokkene een vrije uitdrukkelijke toestemming verleent.

Maar, eén van de vereisten voor een geldige toestemming is dat die toestemming vrij wordt gegeven. Dit betekent dat de klant werkelijk moet kunnen kiezen of hij al dan niet zijn gezondheidsgegevens wil laten verwerken (en dus inzage geeft in zijn vaccinatiebewijs). Als de klant de toegang tot het restaurant, café, vliegtuig of winkel ontzegd wordt omdat hij geen bewijs van vaccinatie wil of kan tonen, dan is die toestemming niet vrij, en kan toestemming niet worden gebruikt als geldige rechtsgrond voor de verwerking.

Er bestaat momenteel geen wettelijke bepaling die dit type van verwerkingen van gezondheidsgegevens zou toestaan.

Kan een organisator van een evenement zoals een festival of een sportevenement mij de toegang weigeren als ik mij niet heb laten vaccineren tegen Covid-19 terwijl ik wel de mogelijkheid daartoe had?

Nee. Een organisator van een evenement mag niet vragen om een vaccinatiebewijs voor te leggen. Het vragen of een persoon al dan niet gevaccineerd is om al dan niet toegang te verlenen tot het evenement, is een verwerking van gezondheidsgegevens. Volgens artikel 9AVG is de verwerking van gezondheidsgegevens in principe verboden, tenzij er een expliciete wettelijke bepaling bestaat die dit toestaat of de betrokkene een vrije uitdrukkelijke toestemming heeft gegeven. Op dit moment bestaat er geen wettelijke bepaling die dit toelaat. Indien een organisator de toegang tot een festivalweide of stadion weigert voor personen die zich niet hebben laten vaccineren, is er ook geen sprake van een 'vrije' toestemming omdat er negatieve gevolgen (met name de weigering van de toegang) verbonden worden aan de weigering van een toestemming.

Kan een werkgever mij om een vaccinatiebewijs vragen?

Nee, de vaccinatiestatus van een persoon is een gezondheidsgegeven. Gezondheidsgegevens zijn een bijzondere categorie van persoonsgegevens. Artikel 9.1 AVG verbiedt de verwerking van gezondheidsgegevens, tenzij een uitdrukkelijke uitzondering voorzien in artikel 9.2 AVG van toepassing is. Zo een uitzondering kan een wettelijke bepaling zijn of de vrije uitdrukkelijke toestemming van de betrokkene. Dit betekent dat de werknemer werkelijk moet kunnen kiezen of hij al dan niet zijn gezondheidsgegevens wil laten verwerken. In de relatie tussen werknemer en werkgever is de toestemming van de werknemer zelden vrij omdat een werknemer grote druk kan ondervinden om toe te stemmen. Meer informatie over Covid-19 op de werkvloer vindt u op deze link.

De GBA heeft verder ook nog geen kennis genomen van enige wettelijke bepaling of CAO die het mogelijk maakt om dit type van verwerkingen van gezondheidsgegevens toe te staan.

Kan mijn werkgever aan alle werknemers vragen of ze gevaccineerd zijn om te kunnen voldoen aan de wettelijke verplichtingen van veiligheid en gezondheid op het werk?

Neen. De werkgever heeft in de Arbeidsovereenkomstenwet een wettelijke verplichting om als een goed huisvader te zorgen dat de arbeid wordt verricht in behoorlijke omstandigheden met betrekking tot de veiligheid en gezondheid van zijn werknemers. Een werkgever mag op basis van deze wettelijke verplichting echter niet aan zijn werknemers vragen wie zich heeft laten vaccineren en wie niet.

Het louter opvragen van deze informatie is al een verwerking van persoonsgegevens, in dit geval zelfs gezondheidsgegevens, onder de AVG. Op de verwerking van gezondheidsgegevens geldt een principieel verbod neergelegd in artikel 9.1 AVG. Op dit verbod bestaan enkele uitzonderingen waardoor de verwerking van deze gezondheidsgegevens rechtmatig is. Zo mogen

gezondheidsgegevens verwerkt worden indien dit noodzakelijk is met het oog op de uitvoering van verplichtingen van de verwerkingsverantwoordelijke (in dit geval de werkgever) op het gebied van het arbeidsrecht en het socialezekerheids- en socialebeschermingsrecht. De GBA is echter van mening dat de verplichtingen van de Arbeidsovereenkomstenwet die op de werkgever rusten geen uitzondering vormen op het principiële verbod van de verwerking van gezondheidsgegevens omdat deze geen voldoende garanties bieden voor een rechtmatige verwerking van gezondheidsgegevens.

Kan een werkgever aan de arbeidsgeneesheer vragen welke werknemers zich hebben laten vaccineren tegen Covid-19?

Neen, dit mag niet. Dit zou niet alleen de bescherming van de persoonsgegevens van de werknemers schenden, maar ook het beroepsgeheim van de arbeidsgeneesheer indien deze gegevens van medische dossiers zou meedelen aan de werkgever.

Er is tot op heden geen wettelijke basis die een uitzondering maakt op het verwerkingsverbod van gezondheidsgegevens of het beroepsgeheim van de arbeidsgeneesheer in de vaccinatiecontext. De werkgever kan dit ook niet doen op basis van een toestemming door de werknemer, omdat dit enerzijds door de precaire relatie tussen de werkgever en werknemer niet beschouwd zal worden als een ‘vrije toestemming’ en omdat anderzijds de toestemming geen uitzondering vormt op het beroepsgeheim van de arbeidsgeneesheer.

Kan een school of universiteit leerlingen of studenten de toegang tot leslokalen verbieden indien ze zich niet hebben laten vaccineren tegen Covid-19?

Neen, dit kan niet. Scholen en universiteiten willen zoveel mogelijk de gezondheid van de leerlingen, studenten en lesgevers garanderen door les te geven in zo veilig mogelijke omstandigheden. Dit verantwoordt echter niet dat ze de toegang tot de leslokalen mogen weigeren voor niet-gevaccineerde leerlingen of studenten. De huidige vaccinatiestrategie bepaalt dat personen niet verplicht zijn om zich te laten vaccineren, maar dit vrij kiezen. Leerlingen of studenten laten bewijzen dat ze zich hebben gevaccineerd voordat ze een leslokaal mogen betreden zou een onrechtmatige verwerking van gezondheidsgegevens inhouden.

Ook indien de toestemming van de betrokken leerlingen of studenten verkregen wordt, zal dit nog steeds verboden zijn. Deze toestemming zal namelijk niet vrij gegeven worden omdat er nadelige gevolgen verbonden worden aan de weigering tot toestemming, namelijk het niet kunnen betreden van de leslokalen.

Tot op heden heeft de GBA ook nog geen kennis genomen van enige wettelijke of decretale bepaling die het mogelijk maakt voor scholen of universiteiten om vaccinatiebewijzen op te vragen met het oog op het creëren van een veilige leeromgeving voor leerlingen en studenten.

Kan men mij dwingen om eerst een medische vragenlijst in te vullen of een medisch attest af te leveren, alvorens ik vrijwilligerswerk mag verrichten (bijv. in een woonzorgcentrum)?

Neen. De Autoriteit stelt vast dat sommige woonzorgcentra vragen om gezondheidsgegevens te delen in de vorm van een vragenlijst of een medisch attest als voorwaarde voor het opnemen van een engagement als vrijwilliger.

Het gaat hier om een inzameling van gezondheidsgegevens van de vrijwilliger. Onder de AVG gelden hiervoor strengere regels. Er geldt een principieel verbod op de verwerking van gezondheidsgegevens, met niettemin enkele limitatieve uitzonderingen op dat verbod, o.a. op grond van de uitdrukkelijke toestemming van de vrijwilliger.

Maar als de voorziening een toestemming vraagt rijst de vraag of een vrijwilliger wel een geldige, vrije toestemming kan geven. Een vrijwilliger kan zich onder druk gezet voelen om toestemming te geven, terwijl de AVG een vrije toestemming vereist. Een vrije toestemming vereist dat de vrijwilliger geen nadelig gevolg mag ondervinden indien hij of zij weigert om het formulier in te vullen (bijv. weigering om de vrijwilliger toe te laten).

Het woonzorgcentrum mag een vrijwilliger dus niet dwingen om een medische vragenlijst in te vullen of een medisch attest af te leveren als voorwaarde om vrijwilligerswerk te verrichten.

Mag ik de verplichte registratiegegevens van bezoekers in een rusthuis nadien hergebruiken om deze bezoekers andere diensten aan te bieden (bijv. een nieuwsbrief of reclame voor ondersteunende diensten toesturen, etc. …)?

Neen, dit mag niet. Momenteel schrijven de bevoegde overheden voor om het bezoek in een rusthuis te registreren.

de richtlijnen van de Vlaamse regering
de richtlijnen van de Waalse regering

de instructies van Iriscare voor de door de GGC erkende rust- en verzorgingstehuizen in Brussel

De registratie van deze persoonsgegevens (naam, adres, telefoonnummer en band met de bewoner) maken deel uit van een veiligheidsmaatregel in de strijd tegen de verspreiding van het COVID-19 virus.

In de eerste plaats moeten woonzorgcentra rekening houden met het beginsel van de minimale gegevensverwerking. Dit betekent dat alleen de persoonsgegevens die noodzakelijk zijn om personen op tijd te kunnen verwittigen bij een besmetting mogen verwerkt worden.

In de tweede plaats moeten woonzorgcentra het beginsel van doelbinding respecteren. Dit betekent dat u de ingezamelde persoonsgegevens (zoals bijv. e-mailadressen) later niet zomaar voor een ander doeleinde, zoals bijv. direct marketing, mag hergebruiken. De bezoeker kan immers niet redelijkerwijze voorzien dat zijn of haar contactgegevens in het kader van de registratieplicht voor een veilig bezoek, zullen hergebruikt worden voor dit ander doeleinde.

Het is volgens de Autoriteit dan ook niet mogelijk de persoonsgegevens van geregistreerde bezoekers te gebruiken voor een ander doel dan voor de bezoekregeling.

Indien de verplichte bezoekersregistratie in de toekomst wordt ingetrokken, moeten de ingezamelde persoonsgegevens bovendien ook verwijderd worden ingevolge artikel 5.1.e) AVG omdat het beoogde doeleinde is bereikt.