contrast

HR • APRIL 2020

Antivirusmaatregelen op de werkvloer.

Wat u moet weten.

De uitbraak van Covid-19 vereist dat u als werkgever maatregelen neemt om een mogelijke verspreiding van het virus op de werkvloer te vermijden.

In dat kader verwerkt u nu mogelijk bijkomende persoonsgegevens over uw werknemers (bijvoorbeeld over recente reizen, hun medische achtergrond, eventuele ziekteverschijnselen).

Het Europees Comité voor gegevensbescherming wijst er echter op dat dit niet zomaar kan zonder inachtneming van de regels inzake gegevensbescherming. Zo dient u een *rechtmatige grondslag* te hebben voor deze verwerking (voor meer informatie zie GDPR toolkit - rechtmatige grondslagen). In België bestaat er volgens de Belgische Gegevensbeschermingsautoriteit momenteel geen reden voor een ruimere of systematische toepassing van de grond vervat in artikel 6.1, d) GDPR (*"noodzaak van de verwerking voor de bescherming van de vitale belangen van de betrokkene of andere natuurlijke personen"*). Voor gezondheidsgegevens wijst de autoriteit bovendien op het verwerkingsverbod van artikel 9 GDPR, waardoor de uitdrukkelijke toestemming van de betrokkene vereist is. De autoriteit wijst er op dat de uitzondering op deze regel om redenen van volksgezondheid enkel geldt indien u handelt *"in uitvoering van uitdrukkelijke richtlijnen opgelegd door de bevoegde overheden"*. In andere landen heeft u misschien omwille van het nationale recht/de nationale maatregelen meer opties. Verder vereist het *beginsel van dataminimalisatie* dat u ook in deze omstandigheden niet meer gegevens verwerkt dan noodzakelijk en het *transparantiebeginsel* dat u de betrokkenen informeert, in het bijzonder over het verwerkingsdoeleinde en de bewaartermijn van de gegevens (voor meer informatie zie GDPR toolkit - transparantie).

Daarnaast probeert u uw werknemers wellicht zoveel mogelijk te laten telewerken. Telewerk wordt aanbevolen in de strijd tegen het Covid-19 virus, maar verhoogt op zijn beurt het risico op digitale virussen. Werknemers gebruiken persoonlijke laptops met een minder goede antivirussoftware en connecteren met het bedrijf via een minder beveiligde internetconnectie. In België waarschuwt het Centrum voor Cybersecurity ook voor de vele phishingberichten die de actualiteit rond het Covid-19 virus misbruiken. Bijkomende maatregelen zijn dus vereist om aan uw beveiligingsverplichting te voldoen en datalekken te vermijden.

contrast

Wat u moet doen.

Probeer de verwerking van (gevoelige) persoonsgegevens zoveel mogelijk te vermijden. Volgens de autoriteit beletten de regels inzake gegevensbescherming bijvoorbeeld niet dat u de lichaamstemperatuur van uw werknemers gaat controleren (zolang deze controle niet gepaard gaat met een registratie van deze gegevens). In dezelfde zin zou het ook toelaatbaar moeten zijn dat u uw werknemers een medische vragenlijst laat invullen voor zover de anonimiteit van de antwoorden kan verzekerd worden.

Voor elke verwerking van persoonsgegevens in de strijd tegen het Covid-19 virus is de (uitdrukkelijke) toestemming van de werknemer vereist. U kan werknemers dus wel *vragen* om elke informatie die in dat kader relevant kan zijn te willen melden, zonder hen daartoe te verplichten. Verder is het aangewezen om één centrale contactpersoon aan te duiden die de betrokken informatie ontvangt en de informatie niet onnodig te verspreiden binnen het bedrijf (bijvoorbeeld enkel aan werknemers die nauw hebben samengewerkt met de betrokkene). In de meeste gevallen zal het niet nodig zijn om de identiteit van de betrokkene te vermelden. Beperk de gegevens in elk geval tot een minimum en bewaar deze niet langer dan nodig voor de bestrijding van deze pandemie. Informeer uw werknemers over de verwerking via een specifiek bericht op het intranet of per e-mail.

Zorg verder dat u telewerk op een veilige manier organiseert. Laat werknemers zoveel mogelijk werken met beveiligde laptops en geëncrypteerde USB-sticks van het bedrijf. Zorg voor een optimaal beveiligde VPN-verbinding en multifactor authentication. Vraag uw werknemers om erop toe te zien dat de (antivirus)software steeds up-to-date is, geregeld back-ups te nemen en bijzonder voorzichtig te zijn bij het openen van bijlagen bij e-mails en hyperlinks. In het licht van de verantwoordingsplicht van uw onderneming, is het aangewezen om deze regels inzake telewerk op te nemen in uw beveiligingsbeleid.