Privacy op de werkvloer en gegevensbescherming

Gids voor militanten

Privacy op de werkvloer en gegevensbescherming.indd 1 2/03/23 09:13

Inleiding

Privacy en gegevensbescherming, een vakbondsthema?

Niet enkel in onze maatschappij neemt de digitalisering toe: denk maar aan de opmars van artificiële intelligentie die massaal data verzamelen. Maar ook op de werkvloer zijn gegevensbescherming en privacy thema's die steeds belangrijker worden. In deze brochure onderzoeken we de impact van de wetgeving over gegevensbescherming op de werkvloer. Eerst geven we een overzicht van de wetgeving. Daarna staan we stil bij hoe ze wordt toegepast in het kader van de arbeidsverhoudingen tussen de werkgever en zijn werknemers. We onderzoeken welke gegevens er mogen worden verwerkt, onder welke voorwaarden en welke wettelijke beperkingen er zijn bij de controle en het toezicht op werknemers. Tot slot bestuderen we de (eventuele) impact van de wetgeving op het syndicale werk en de taken van de vakbondsvertegenwoordigers.

Voor bijkomende informatie verwijzen we naar de referentiewebsite voor alle vragen over privacy en gegevensbescherming op de werkvloer: die van de Gegevensbeschermingsautoriteit (GBA), een onafhankelijk orgaan dat erop toeziet dat de grondbeginselen van de bescherming van de persoonsgegevens worden nageleefd. Dit orgaan is de opvolger van de voormalige Privacycommissie.
https://www.gegevensbeschermingsautoriteit.be/

Je kan ook informatie aanvragen over een specifiek geval in het kader van je werk : **Informatie aanvragen | Gegevensbeschermingsautoriteit**

En tot slot kan je ook terecht op de website van het ACV, waar je op **www.hetacv.be/privacy** een antwoord op de meest gestelde vragen kan vinden.

Privacy op de werkvloer en gegevensbescherming.indd 3 2/03/23 09:13

Inhoudstafel

I. Wetgeving over gegevensbescherming **6**

1. Privacy en gegevensbescherming 7
2. Wat wordt er verstaan onder « persoonsgegevens » ? 7
3. GDPR : algemene beginselen 8
4. De rechten van de betrokkenen 10
5. Verplichtingen voor verwerkingsverantwoordelijken 11
6. Verwerking van gevoelige gegevens 13

II. Privacy op de werkvloer **14**

1. Voorwaarden voor de verwerking van werknemersgegevens en verplichtingen van de werkgevers 15
   - 1.1 Verwerking van werknemersgegevens 15
   - 1.2 Verwerking van gezondheidsgegevens 17
   - 1.3 Verplichtingen voor de werkgevers 17
   - 1.4 Hoe kan ik mijn rechten doen gelden ? 18
2. Controle en toezicht op de werkvloer: basisprincipes 20
   - 2.1 Camerabewaking op de arbeidsplaats: cao nr. 68 21
   - 2.2 Controle op de elektronische onlinecommunicatiegegevens: cao nr. 81 22
   - 2.3 Controle van de werknemers bij vermoeden van diefstal: cao nr. 89 24
   - 2.4 Geolocalisatie 25
   - 2.5 Cao nr. 38 betreffende de werving en selectie van werknemers 27

III. Gegevensbescherming en vakbondswerk **28**

1. Persoonsgegevens en lidmaatschap 29
2. Gebruik van persoonsgegevens door vakbondsvertegenwoordigers 29
3. Impact van de GDPR op het sociaal overleg 30
4. Controleren of de werkgever de GDPR respecteert 33

Privacy op de werkvloer en gegevensbescherming.indd 5 2/03/23 09:13

I. Wetgeving over gegevensbescherming

1. Privacy en gegevensbescherming

De huidige privacywet in België dateert al van 1992. Als gevolg van een aantal veranderingen spreekt men voortaan van persoonsgegevens in het kader van privacy. Persoonsgegevens zijn concreter en bestaan uit specifieke informatie. Dit maakt het makkelijker om concrete regelgeving hierover op te stellen.

De basiswetgeving over gegevensbescherming is nu vooral Europese regelgeving. De **GDPR** (General Data Protection Regulation) of Algemene Verordening Gegevensbescherming ging in 2018 van kracht en is van toepassing op alle EU-burgers en alle openbare en privéorganisaties die persoonsgegevens verwerken op het grondgebied van de Europese Unie.

De wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens bracht de Belgische wetgeving over gegevensbescherming in overeenstemming met de GDPR en legde een aantal open clausules uit de GDPR ten uitvoer.

2. Wat zijn « persoonsgegevens » ? (artikel 4.1 van de GDPR)

Persoonsgegevens zijn alle informatie over een natuurlijke persoon die direct of indirect kan worden geïdentificeerd.

Enkele voorbeelden zijn : naam, voornaam, geboortedatum, adres, rijksregisternummer, locatiegegevens (GPS-gegevens), online ID's, specifieke elementen die kenmerkend zijn voor de fysieke, fysiologische (bv. grootte, gewicht, ...), economische of sociale identiteit (loon, gehuwd zijn, kinderen hebben, ...).

Er wordt een onderscheid gemaakt tussen twee gegevenscategorieën: de zogenaamde gewone gegevens en de **gevoelige** gegevens (zogenaamde bijzondere categorieën van persoonsgegevens, art. 9 GDPR). We komen daar verder op terug.

Privacy op de werkvloer en gegevensbescherming.indd 7 2/03/23 09:13

3. GDPR : algemene beginselen (art. 5-6 GDPR)

De GDPR beschermt de persoonsgegevens van alle Europese burgers door de gegevensverwerking aan bepaalde voorwaarden te koppelen.

Onder « *verwerking* » wordt verstaan: een bewerking of een geheel van bewerkingen (al dan niet uitgevoerd via geautomatiseerde processen) met betrekking tot persoonsgegevens of een geheel van persoonsgegevens. De organisatie of persoon die de verwerking uitvoert is de *verwerkingsverantwoordelijke*.

Regeringen, vakbonden en ondernemingen[1] zullen dus worden beschouwd als «*verwerkingsverantwoordelijken*», nl. organisaties die persoonsgegevens moeten verwerken.

Voorbeelden van verwerkingsactiviteiten zijn : het verzamelen, vastleggen, opslaan, wijzigen, opvragen, raadplegen, gebruiken, doorsturen, verspreiden of op andere wijze ter beschikking stellen, wissen of vernietigen van persoonsgegevens.

Bij de verwerking van persoonsgegevens gelden zes basisbeginselen:

1) Ten eerste moet **de verwerking rechtmatig**, behoorlijk en transparant zijn.

   De verwerking is alleen rechtmatig (= toegestaan) voor zover (ten minste) aan een van de zes onderstaande voorwaarden is voldaan:

   - **De betrokkene heeft toestemming gegeven:** de betrokkene moet expliciet en duidelijk toestemming geven om de persoonsgegevens te verwerken voor een of meerdere specifieke doeleinden. In artikel 4 en 7 van de GDPR wordt verduidelijkt dat de toestemming tegelijkertijd vrij, specifiek, geïnformeerd en ondubbelzinnig moet zijn. Dat betekent dat de toestemming bijvoorbeeld niet gebonden kan zijn aan de sluiting van een (vrije) overeenkomst, dat ze voor één of meerdere specifieke doeleinden gevraagd moet worden, dat de personen voldoende ingelicht (voorgelicht) worden en dat de toestemming moet voortvloeien uit een duidelijke positieve handeling[2] (ondubbelzinnig). De toestemming kan op elk ogenblik worden ingetrokken.

[1] *We gebruiken in deze brochure de term onderneming(en) om te verwijzen naar bedrijven, (zorg)instellingen, organisaties,...*

[2] *Indien iemand niet antwoordt op een e-mail waarin de toestemming van de persoon gevraagd wordt, kunnen we er dus niet van uitgaan dat die persoon bijvoorbeeld zijn toestemming heeft gegeven.*

Privacy op de werkvloer en gegevensbescherming.indd 8 2/03/23 09:13

In het kader van een arbeidsverhouding vormt toestemming geven een probleem omdat de werknemers hiërarchisch ondergeschikt zijn aan hun werkgever. We komen hier verderop op terug.

De andere rechtsgrondslagen hieronder laten toe om persoonsgegevens te verwerken zonder toestemming van de betrokkene.

- **De verwerking is noodzakelijk voor de uitvoering van een overeenkomst:** bv. de arbeidsovereenkomst waarbij gegevens moeten worden verzameld om het loon te kunnen uitbetalen.
- **De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting** (bv. wanneer een onderneming verwerkingsverantwoordelijke is, is ze onderworpen aan een aantal verplichtingen op het vlak van welzijn op het werk waarbij persoonsgegevens moeten worden verwerkt).
- **De verwerking is noodzakelijk om de vitale belangen van de betrokkene te beschermen** (bv.: medische context waarbij het leven van de betrokkene op het spel staat).
- **De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of in het kader van de uitoefening van het algemeen gezag** (bv. een gemeente moet gegevens verzamelen om een bewonerskaart te kunnen toekennen).
- **De verwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang van de verwerkingsverantwoordelijke,** behalve wanneer de belangen of de fundamentele vrijheden en grondrechten van de betrokkene zwaarder wegen (bv. verwerking om de computerbeveiliging te waarborgen of fraude te voorkomen).

2) De **verwerking moet plaatsvinden voor een welbepaald, uitdrukkelijk omschreven doeleinde.** De betrokken gegevens mogen in principe niet worden gebruikt voor een ander dan het oorspronkelijk opgegeven doeleinde. Deze gegevens mogen enkel voor een ander doeleinde worden gebruikt als werd nagegaan of het nieuwe doeleinde verenigbaar is met het oorspronkelijke doeleinde.

3) De **gegevensverwerking moet minimaal zijn :** dit betekent dat enkel gegevens worden gebruikt die echt noodzakelijk zijn voor het beoogde doeleinde.

4) De **verwerkte gegevens moeten juist zijn** en zo nodig worden geactualiseerd. Als de persoonsgegevens onjuist zijn, moeten ze worden gewist of gecorrigeerd.

5) De **gegevensopslag moet beperkt zijn.** Die hangt af van het doeleinde en de (min of meer lange) periode waarin de gegevens nodig zijn.

Privacy op de werkvloer en gegevensbescherming.indd 9 2/03/23 09:13

6) Tot slot moeten er **passende technische of organisatorische maatregelen worden getroffen** om de beveiliging van de persoonsgegevens te waarborgen.

4. De rechten van de betrokkenen (art. 12-22 GDPR)

De GDPR kent burgers een aantal rechten toe in verband met hun gegevens:

1. **Transparantie:** de verwerkingsverantwoordelijke moet de betrokkene op beknopte, transparante en begrijpelijke wijze inlichten over de verwerking van zijn gegevens. De informatie moet bestaan uit:
   - de doeleinden van de verwerking;
   - de rechtsgrond van de verwerking ;
   - de categorieën van ontvangers van de gegevens ;
   - de identiteit en de contactgegevens van de verwerkingsverantwoordelijke;
   - het bestaan van bepaalde rechten voor de betrokkene (zie punt 2 tot 8).
2. **Toegangsrecht:** de betrokkenen hebben het recht om te weten welke persoonsgegevens er worden verwerkt, wat de doeleinden van de verwerking zijn, wie de ontvangers van de gegevens zijn en hoe lang de gegevens worden opgeslagen. De betrokkene heeft het recht om gratis een kopie van de verwerkte persoonsgegevens te ontvangen.
3. **Recht op rectificatie:** de betrokkene heeft het recht om vervollediging of rechtzetting van onvolledige of onjuiste persoonsgegevens te verkrijgen.
4. **Recht op gegevenswissing** (« recht om vergeten te worden»): de betrokkene heeft het recht om aan de verwerkingsverantwoordelijke de verwijdering van persoonsgegevens te verkrijgen onder bepaalde voorwaarden, bv. als de gegevens niet langer nodig zijn, als de betrokkene de toestemming intrekt, bezwaar maakt tegen de verwerking of als de gegevens onrechtmatig verwerkt zijn (zie art. 17 GDPR).
5. **Recht op beperking van de verwerking:** op vraag van de betrokkene moet een organisatie de verwerking van de persoonsgegevens stopzetten, bv. als de betrokkene de juistheid van de persoonsgegevens betwist of als de verwerking onrechtmatig is (zie art. 18 GDPR).

Privacy op de werkvloer en gegevensbescherming.indd 10 2/03/23 09:13

De verwerkingsverantwoordelijke stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt in kennis van elke rechtzetting of verwijdering van persoonsgegevens of beperking van de verwerking.

6. **Recht op overdraagbaarheid van gegevens:** het is mogelijk een deel van je gegevens in een geautomatiseerde leesbare vorm te verkrijgen om ze voor eigen doeleinden te kunnen gebruiken.
7. **Recht van bezwaar:** de betrokkene kan bezwaar maken tegen een verwerking wanneer die stoelt op gerechtvaardigde belangen (van de verantwoordelijke) of nodig is voor uitoefening van een taak van algemeen belang. Behalve in geval van direct marketing moet de betrokkene « met zijn specifieke situatie verband houdende redenen » aanvoeren. De verantwoordelijke kan echter de verwerking voortzetten als hij kan aantonen dat er dwingende gerechtvaardigde gronden zijn die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.
8. De betrokkene moet **het recht hebben niet te worden onderworpen aan een louter op geautomatiseerde verwerking** gebaseerd besluit waaraan rechtsgevolgen zijn verbonden of dat hem « op vergelijkbare wijze » aanmerkelijk treft (behoudens uitzonderingen, zie art. 22 GDPR).

   Een geautomatiseerd besluit is een besluit dat werd genomen door een algoritme, zonder menselijke tussenkomst. Zo kan bijvoorbeeld de toekenning of weigering van een krediet uitsluitend worden gebaseerd op de beslissing van een algoritme dat automatisch bepaalde criteria toepast op de financiële situatie van de aanvrager, zonder menselijke tussenkomst.

5. Verplichtingen voor verwerkingsverantwoordelijken (art. 24-37 GDPR)

Personen of organisaties die gegevens verwerken (= verwerkingsverantwoordelijken) moeten een aantal verplichtingen nakomen:

- Passende technische en organisatorische maatregelen treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming is met de GDPR.
- Wanneer er een beroep wordt gedaan op verwerkers, enkel met verwerkers samenwerken die afdoende garanties bieden met be-

Privacy op de werkvloer en gegevensbescherming.indd 11 2/03/23 09:13

trekking tot het toepassen van passende technische en organisatorische maatregelen. De gegevensverwerking door een verwerker moet worden geregeld in een overeenkomst of een wetsbesluit die bepaalde elementen moet bevatten die omschreven worden in art. 28 van de GDPR.

- Ervoor zorgen dat de betrokkene zijn rechten gemakkelijker kan uitoefenen.
- Een register van alle verwerkingsactiviteiten bijhouden, dat de volgende gegevens bevat: de naam en de contactgegevens van de verwerkingsverantwoordelijke(n), de verwerkingsdoeleinden, een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens, de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist en een algemene beschrijving van de beveiligingsmaatregelen.
- Meewerken met de toezichthoudende autoriteit bij het vervullen van haar taken.
- Doeltreffende beveiligingsprocedures toepassen. Dit wil zeggen dat er informaticamaatregelen moeten worden getroffen om gegevenslekken te vermijden, gegevens te pseudonimiseren of versleutelen of uit voorzorg het aantal personen te beperken die toegang hebben tot deze persoonsgegevens.
- Een inbreuk in verband met persoonsgegevens die een risico inhoudt voor de rechten en vrijheden van natuurlijke personen melden aan de Gegevensbeschermingsautoriteit. Deze melding moet zo snel mogelijk plaatsvinden, indien mogelijk binnen de 72 uur na kennisname. Als de inbreuk een hoog risico inhoudt voor de rechten en de vrijheden van een natuurlijke persoon, moet de verwerkingsverantwoordelijke ze zo snel mogelijk aan de betrokkene melden.
- Een beoordeling uitvoeren van het effect wanneer de gegevensverwerking een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen.
- Een functionaris voor gegevensbescherming (DPO) aanwijzen wanneer aan bepaalde voorwaarden is voldaan (zie artikel 37 GDPR).

Privacy op de werkvloer en gegevensbescherming.indd 12 2/03/23 09:13

6. Verwerking van gevoelige gegevens (art. 9 GDPR)

De GDPR vermeldt een bijzondere categorie van gegevens : de gevoelige gegevens. Volgens de GDPR gaat het om persoonsgegevens waaruit de etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen of het lidmaatschap van een vakbond blijken. Daarnaast gaat het ook om genetische gegevens, biometrische gegevens of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

In principe is het verboden om deze gegevens te verwerken, maar er bestaan uitzonderingen. Deze gegevens mogen worden verwerkt als de betrokkene (uitdrukkelijke) toestemming heeft gegeven of, als de toestemming er niet is, als de verwerking noodzakelijk is om een wettelijke verplichting na te leven (ongeacht of het een wet of een collectieve arbeidsovereenkomst betreft, bv. op het vlak van arbeidsrecht) of als de verwerking nodig is voor doeleinden van arbeidsgeneeskunde bijvoorbeeld.

Privacy op de werkvloer en gegevensbescherming.indd 13 2/03/23 09:13

II. Privacy en gegevensbescherming op de werkvloer

1. Voorwaarden voor de verwerking van werknemersgegevens en verplichtingen van de werkgevers

De GDPR komt boven op de bestaande bepalingen die op de arbeidsrelatie van toepassing zijn en versterkt de verplichtingen van de werkgever. Hoewel de doelstelling van de GDPR is om de regels voor gegevensbescherming binnen de EU te harmoniseren, voorziet de verordening in een uitzondering voor arbeidsrelaties. Het is dus mogelijk om specifieke regels vast te leggen voor de verwerking van persoonsgegevens van werknemers, zowel op sectoraal als op bedrijfsniveau, bijvoorbeeld via collectieve arbeidsovereenkomsten (artikel 88 GDPR).

1.1 Verwerking van werknemersgegevens

Op het werk worden de persoonsgegevens van alle werknemers op verschillende momenten verwerkt. Meestal gebeurt dat onder één van de volgende voorwaarden:

1. De **werknemers hebben hun (individuele) toestemming gegeven.**

   Laten we eens stilstaan bij de bijzonderheid van deze rechtsgrondslag in het kader van de arbeidsrelatie. Aangezien de werknemer ondergeschikt is, werd er geoordeeld dat die moeilijk uit vrije wil zijn toestemming kan geven. Deze vrije wil is echter een voorwaarde om de toestemming als geldig te beschouwen. Het is dan ook zeer riskant voor een werkgever om de specifieke verwerking van werknemersgegevens uitsluitend op basis van hun toestemming te rechtvaardigen. De werkgever moet zich op een andere rechtsgrondslag kunnen baseren.
2. De **verwerking is noodzakelijk om een overeenkomst (de arbeidsovereenkomst) uit te voeren.**
3. De **verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting.** Dit is het geval wanneer een wet, een decreet, een ordonnantie of een cao voorschrijft dat persoonsgegevens moeten worden verwerkt om aan die wet, dat decreet, een ordonnantie of die cao te voldoen.

In een onderneming zijn persoonsgegevens ofwel nominatieve gegevens, d.w.z. informatie die niet anoniem is en rechtstreeks verband houdt met een werknemer, ofwel niet-nominatieve gegevens op basis waarvan je een werknemer indirect kan identificeren.

Privacy op de werkvloer en gegevensbescherming.indd 15 2/03/23 09:13

Mogelijke rechtsgrondslagen voor de verwerking van persoonsgegevens van werknemers zonder hun toestemming:

- Uitvoeren van een (arbeids)overeenkomst

  Bv.: gegevens die nodig zijn om het loon of uitkeringen te betalen, in het kader van arbeidsongeschiktheid, enz.

  - gezinssamenstelling, rekeningnummer, adres, enz.
- Naleven van een wettelijke verplichting

  Bv.: verwerken van gegevens die bestemd zijn voor een sociale-zekerheidsinstelling tijdens een aanwerving (Dimona-aangifte).
- Nastreven van het legitieme belang van de werkgever, vaak de goede werking van de onderneming.
  Bv.: verwerken van persoonsgegevens om de toegang tot gebouwen te beveiligen.

Indien een van deze rechtsgrondslagen wordt nageleefd, heeft de werkgever de toestemming van de werknemers niet nodig, maar moet hij de transparantieplicht wel naleven. De werkgever moet de werknemers informeren over het soort gegevens dat zal worden verzameld.

Voor de verwerking van gegevens in andere gevallen heeft hij wel de toestemming van de werknemers nodig.

Bv.: foto's van werknemers verspreiden op het intranet of de site van de onderneming. Hierbij mag hij de uitvoering van het contract, een wettelijke verplichting of de goede werking van de onderneming niet als reden inroepen. De toestemming van elk individu is dus vereist.

Een voorbeeld waarbij verwerking van gegevens verboden is: lidmaatschap van een vakbond

Het lidmaatschap van een vakbond is een gevoelig gegeven. Een werkgever heeft niet het recht om te vragen of je lid bent van een vakbond. Deze vraag is strijdig met de GDPR.

Er is geen enkele wet die een werkgever toestaat te vragen of je lid bent van een vakbond. Er is ook geen reden en geen belang bij om te antwoorden.

Privacy op de werkvloer en gegevensbescherming.indd 16 2/03/23 09:13

1.2 Verwerking van gezondheidsgegevens

De GDPR verbiedt in principe de verwerking van gezondheidsgegevens, die als "gevoelig" worden beschouwd. **Een werkgever heeft dus geen toegang tot medische gegevens.** Niet tijdens de aanwerving en ook niet tijdens de arbeidsrelatie.

Een werkgever mag een sollicitant niet vragen naar zijn of haar gezondheidstoestand. Het is namelijk verboden om iemand te discrimineren op basis van zijn huidige of toekomstige gezondheidstoestand. De toekomstige werknemer is dan ook niet verplicht om vragen over zijn gezondheidstoestand te beantwoorden. Het is de plicht van de werkgever om alle nodige maatregelen te treffen voor de gezondheid en het welzijn van zijn werknemers op de werkvloer. De arbeidsarts heeft dan weer als taak om de gezondheid van de (toekomstige) werknemers te onderzoeken en te beslissen of zij (nog) geschikt zijn om hun job uit te oefenen. De arbeidsarts moet de werkgever enkel informeren of een werknemer al dan niet arbeidsgeschikt is, zonder ooit informatie te geven over een mogelijke ziekte of aandoening.

Wanneer een werknemer ziek is, moet de werkgever op de hoogte worden gebracht van de afwezigheid om medische redenen. Hij hoeft de precieze reden echter niet te kennen en heeft ook geen toegang tot informatie van de behandelende arts of de adviserend arts. De werknemer is verplicht om een medisch attest voor een afwezigheid van meer dan één dag in te dienen als het arbeidsreglement van de onderneming of een cao daarin voorziet. In andere gevallen moet de werkgever er telkens om vragen. Artikel 31 van de Arbeidsovereenkomstenwet van 1978 bepaalt welke gegevens er op een medisch attest moeten vermeld staan, onder andere de duur van de arbeidsongeschiktheid. De diagnose wordt echter nooit vermeld omdat deze onder het medisch beroepsgeheim valt. In het deel dat voorbehouden is voor de controledienst staat de diagnose wel. Dat is in overeenstemming met de GDPR, die in een uitzondering voorziet op het verbod om dit soort gegevens te verwerken aangezien het om een wettelijke verplichting gaat volgens het arbeidsrecht (voor meer informatie, zie titel 4 van boek I van de Codex over het welzijn op het werk).

1.3 Verplichtingen voor werkgevers

De GDPR verplicht de werkgever, die verantwoordelijk is voor de verwerking, om de volgende informatie aan de werknemer te bezorgen:

- de **periode waarin de persoonsgegevens worden bewaard** of, indien dat niet mogelijk is, de criteria die worden gehanteerd om deze

Privacy op de werkvloer en gegevensbescherming.indd 17 2/03/23 09:13

periode te bepalen (in principe worden sociale documenten 5 jaar bewaard vanaf het einde van de arbeidsovereenkomst);

- indien de werknemer zijn toestemming heeft gegeven om zijn gegevens te verwerken, **het recht om die toestemming op elk ogenblik in te trekken;**
- het recht om een **klacht in te dienen bij de gegevensbeschermingsautoriteit.**

Deze informatie moet niet volgens een specifieke vormvereiste meegedeeld worden, maar wordt bij voorkeur wel in het arbeidsreglement opgenomen. Zo wordt ze paritair opgesteld, met de inbreng van de vakbondsvertegenwoordigers in de sociale overlegorganen.

Als verwerkingsverantwoordelijke moet **de werkgever ook een register bijhouden van de verwerkte gegevens.** Volgens de GDPR moeten alle ondernemingen met meer dan 250 personen een dataregister bijhouden. Voor kleinere ondernemingen geldt deze verplichting slechts wanneer de verwerking een risico kan inhouden voor de rechten en vrijheden van de betrokkenen, regelmatig gebeurt of over gevoelige gegevens gaat. In de praktijk zal dat in bijna alle ondernemingen het geval zijn. Bovendien is personeelsbeheer volgens de gegevensbeschermingsautoriteit een regelmatige verwerking. De GBA raadt alle bedrijven aan een dataregister bij te houden, ook als deze verplichting niet op hen van toepassing is.

De werkgever moet **de GBA en de betrokken werknemer(s) op de hoogte brengen van elke inbreuk op de persoonsgegevens** en staat toe dat er gegevens worden rechtgezet of gewist.

Ten slotte is de werkgever verplicht **de verwerkte gegevens tot een minimum te beperken,** d.w.z. dat die alleen gegevens mag verwerken die *"toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt".*

Een schending van deze verplichtingen kan leiden tot een boete van maximaal 20.000.000 euro of 4% van de jaarlijkse wereldwijde omzet van de onderneming.

1.4 Hoe kan ik mijn rechten doen gelden (art. 12 GDPR)?

Alle rechten die de GDPR aan de Europese burgers verleent, moeten ook gelden voor werknemers (recht op informatie, om je gegevens in te kijken, om te worden vergeten, om je gegevens aan te passen, enz.). Zoals we eerder hebben gezien, is het de verwerkingsverantwoordelijke, in

Privacy op de werkvloer en gegevensbescherming.indd 18 2/03/23 09:13

dit geval de werkgever, die het makkelijker moet maken voor de werknemers om hun rechten i.v.m. hun persoonsgegevens uit te oefenen.

Wanneer een **werknemer vraagt om een van deze rechten uit te oefenen, moet de verwerkingsverantwoordelijke die persoon** *«zonder onnodige vertraging en in elk geval binnen een maand na ontvangst van het verzoek»* **informeren over het gevolg dat is gegeven aan zijn verzoek.** Deze termijn kan met twee maanden worden verlengd wanneer het om een complex verzoek gaat of wanneer er meerdere werden ingediend. Het verzoek kan worden aanvaard of geweigerd.

Indien de verwerkingsverantwoordelijke geen gevolg geeft aan het verzoek, moet hij de betrokkene daarvan onmiddellijk en uiterlijk binnen een maand op de hoogte brengen en daarbij vermelden waarom het verzoek werd geweigerd. De verwerkingsverantwoordelijke moet de betrokkene ook informeren dat die een klacht kan indienen bij de Gegevensbeschermingsautoriteit en beroep kan aantekenen.

Als je vaststelt dat je werkgever je persoonsgegevens verwerkt op een manier die volgens jou niet correct is, is de eerste stap contact opnemen met de werkgever, zoals hierboven beschreven. Leidt dat tot niets, dan kun je je ook tot de Gegevensbeschermingsautoriteit wenden of gerechtelijke stappen ondernemen.

Maar hoe zit het met de rol van de vakbond in deze context?

Volgens de Belgische wet waarin de GDPR wordt omgezet, kan een vakbondsorganisatie een werknemer niet vertegenwoordigen bij de GBA. Je kunt je als werknemer dus niet officieel laten vertegenwoordigen door het ACV voor de Gegevensbeschermingsautoriteit. Als er daarentegen een probleem ontstaat over gegevens die de werkgever heeft verwerkt, is dat een geschil tussen de werknemer en de werkgever. Bij een individueel geschil heeft iedere werknemer het recht zich te laten bijstaan door zijn vakbondsafgevaardigde (VA). Die komt dan tussen bij de werkgever om de werknemer zijn rechten te verdedigen. In de geest van de wet is de vakbondsafvaardiging dus de gesprekspartner ten opzichte van de werkgever, maar niet ten opzichte van de GBA, zelfs wanneer het gaat om een problematiek omtrent de verwerking van persoonsgegevens.

Volgens art. 12 van cao nr. 5 heeft de vakbondsafvaardiging overigens het recht om met de persoon aan het hoofd van de

Privacy op de werkvloer en gegevensbescherming.indd 19 2/03/23 09:13

onderneming te spreken voor elk geschil of betwisting van collectieve aard dat zich in de onderneming voordoet. Wanneer een gegevensverwerkingsbeleid problematisch is, is de betwisting collectief, en is de VA dus bevoegd. Bijvoorbeeld: wanneer alle werknemers van een onderneming verplicht zouden zijn een document te ondertekenen waarbij de werkgever toestemming krijgt om persoonsgegevens te verzamelen die hij niet mag verwerken.

Kortom, gaat het om een specifieke aangelegenheid, namelijk gegevensbescherming, dan wordt er niet meteen geraakt aan het arbeidsrecht. De vakbondsafvaardiging behoudt haar bevoegdheden: als de rechten van een werknemer worden bedreigd, is de VA bevoegd.

2. Controle en toezicht op de werkvloer: basisprincipes

Hier focussen we op de controle van de werknemers en de mogelijke inmenging in hun privéleven. Verschillende collectieve arbeidsovereenkomsten regelen specifieke gevallen van toezicht op werknemers.

De GDPR bevat drie principes waarmee de werkgever rekening moet houden bij het uitoefenen van toezicht op de werkplek en bij de verwerking van persoonsgegevens van werknemers. Zo wordt de inbreuk op de privacy van werknemers tot een minimum beperkt:

- **Het finaliteitsbeginsel:** het doeleinde waarvoor de controle wordt uitgeoefend, moet legitiem zijn. Deze legitieme doeleinden kunnen worden vastgelegd bij wet of in een van de cao's die betrekking hebben op een specifiek aspect van het toezicht op werknemers.
- **Het evenredigheidsbeginsel:** de controle moet beperkt zijn en in verhouding staan tot het doel. De verwerkte gegevens moeten beperkt blijven tot wat nodig is om het doeleinde van het toezicht te bereiken. Concreet betekent dit dat wanneer gegevens worden verzameld, deze zo algemeen mogelijk moeten worden gehouden en eventueel anoniem moeten worden gemaakt. De individualisering van gegevens, die de identificatie van een bepaalde werknemer mogelijk maakt, zal in beginsel niet worden toegestaan.
- **het transparantiebeginsel:** dit gaat om de verplichting om werknemers te informeren. Dat betekent dat ze moeten wor-

Privacy op de werkvloer en gegevensbescherming.indd 20 2/03/23 09:13

den ingelicht dat hun gegevens worden verwerkt en voor welke doelen. Deze informatie moet worden verstrekt op het moment dat de gegevens worden verzameld, dus bij het sluiten van de arbeidsovereenkomst.

Na de inwerkingtreding van de GDPR komen de bepalingen van de verordening bovenop die van de reeds bestaande cao's die het toezicht op werknemers regelen. We bespreken ze hieronder.

2.1 Camerabewaking op de arbeidsplaats: cao nr. 68

Cao nr. 68 handelt over de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats in de privésector. De toelaatbaarheids- en installatievoorwaarden van de camerabewaking op de arbeidsplaats dienden vastgelegd te worden volgens de drie hierboven genoemde beginselen.

Camerabewaking op de arbeidsplaats is enkel toegelaten voor het nastreven van één van de volgende doeleinden:

- de veiligheid en gezondheid
- de bescherming van de goederen van de onderneming
- de controle van het productieproces (kan betrekking hebben op zowel machines als op de werknemers)

Voor de eerste twee beginselen is de camerabewaking non-stop. Voor het laatste beginsel is voortdurende camerabewaking enkel toegelaten voor machines en tijdelijke camerabewaking voor werknemers.

Dat wil zeggen dat voortdurende camerabewaking van werknemer niet toegelaten is en voortdurende camerabewaking van machines enkel toegelaten in de mate dat het niet de bedoeling is om de werknemer te viseren.

De werkgever dient het doeleinde van de camerabewaking duidelijk en expliciet te omschrijven.

Voorafgaandelijk, én bij het opstarten van de camerabewaking, moet de werkgever de ondernemingsraad over alle aspecten van de camerabewaking informatie verschaffen. Bij gebrek aan een OR wordt deze informatie verschaft aan het Comité PB of, bij het onbreken daarvan, aan de VA of, bij afwezigheid daarvan, aan de werknemers.

Privacy op de werkvloer en gegevensbescherming.indd 21 2/03/23 09:13

De informatie die moet verschaft worden, heeft betrekking op minstens de volgende aspecten van de camerabewaking:

- het nagestreefde doeleinde;
- het feit of de beelden al dan niet bewaard worden;
- het aantal en de plaatsing van de camera's;
- de betrokken periode of periodes gedurende dewelke de camera's functioneren.

De OR of, bij gebrek daaraan, het Comité PB moet bovendien regelmatig de gehanteerde bewakingssystemen evalueren en voorstellen doen met het oog op herziening in functie van de technologische ontwikkelingen.

2.2 Controle op de elektronische onlinecommunicatiegegevens: cao nr. 81

Op grond van de wet over de arbeidsovereenkomsten die het gezag van de werkgever erkent kan **de werkgever in de privésector het gebruik van communicatiemiddelen door de werknemers controleren**, kennisnemen van hun communicatiegegevens en deze persoonsgegevens verwerken.

De voorwaarden van de verwerking zijn bepaald in cao nr. 81, die globale controle op de elektronische onlinecommunicatiegegevens enkel toelaat als de hierboven genoemde beginselen van de GDPR worden nageleefd. Praktisch betekent dit dat **de controle een specifieke doelstelling moet hebben, dat de werkgever niet systematisch alles mag controleren en dat de werknemer moet weten dat de werkgever controle mag uitoefenen.** Dit betekent niet dat de werknemer toestemming moet geven. Hij moet enkel op voorhand worden ingelicht dat controle mogelijk is.

Controle op de elektronische onlinecommunicatiegegevens is enkel toegelaten wanneer een of meerdere van volgende doeleinden worden nagestreefd (dit moet expliciet worden bepaald) :

- het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van een andere persoon kunnen schaden;
- de bescherming van de economische, handels- en financiële belangen van de onderneming die vertrouwelijk zijn en het tegengaan van ermee in strijd zijnde praktijken;
- de veiligheid en/of de goede technische werking van de IT-netwerksystemen van de onderneming, met inbegrip van de controle op de kosten die ermee gepaard gaan en de fysieke bescherming van de installaties van de onderneming;

Privacy op de werkvloer en gegevensbescherming.indd 22 2/03/23 09:13

- het te goeder trouw naleven van de in de onderneming geldende beginselen en regels voor het gebruik van onlinetechnologieën.

De werkgever die een controlesysteem wil installeren **moet eerst de OR, of, bij ontbreken ervan, het Comité PB, of, bij ontbreken ervan, de VA, of,** bij ontbreken ervan, de werknemers inlichten over alle aspecten van de controle. Deze informatie moet gaan over het controlebeleid en de voorrechten van de werkgever, de nagestreefde doelstelling(en), het feit of gegevens al dan niet worden bewaard (en zo ja, de plaats en de duur) en het al dan niet permanente karakter van de controle.

Bij de installatie van het controlesysteem moet **de werkgever de individuele werknemers ook inlichten over alle aspecten van de controle.** Het betreft collectieve informatie en informatie over de volgende aspecten:

- het gebruik van de instrumenten die de werknemer voor de uitvoering van zijn werk ter beschikking worden gesteld, inclusief de beperkingen wat het gebruik in het kader van de functie betreft;
- de rechten, plichten en verplichtingen van de werknemers en de eventuele verboden inzake het gebruik van de elektronische onlinecommunicatiemiddelen van de onderneming;
- de in het arbeidsreglement bepaalde straffen wanneer de regels niet in acht worden genomen.

De werkgever kan kiezen hoe hij de werknemers inlicht : via aanplakking, in het arbeidsreglement of in de arbeidsovereenkomst of door instructies bij gebruik (boodschappen op het scherm wanneer de werkpost wordt aangezet en/of bepaalde programma's worden geactiveerd).

Deze informatie moet niet verplicht in het arbeidsreglement staan, maar het is aanbevolen om in het arbeidsreglement duidelijke regels op te nemen over de elektronische controle op de werkvloer met respect voor het sociaal overleg.

In eerste instantie is het toegelaten om globale gegevens te verzamelen. Identificatie van de werknemers is echter niet toegelaten.

Een aanbeveling van de Gegevensbeschermingsautoriteit stelt dat de werkgever wat internet betreft gegevens kan verzamelen over de duur van de aansluiting per werkpost, maar de bezochte sites niet kan individualiseren. Wat e-mail betreft, kan de werkgever gegevens verzamelen over het aantal per werkpost uitgaande berichten en het volume ervan, maar kan hij de werknemer die ze heeft verstuurd niet identificeren.

Privacy op de werkvloer en gegevensbescherming.indd 23 2/03/23 09:13

Op basis van de informatie die zich op de server bevindt mogen in eerste instantie lijsten met globale gegevens worden opgesteld waarmee geen individuele werknemers kunnen worden geïdentificeerd. Wanneer op basis van die algemene lijsten onregelmatigheden vermoed worden, wordt de werknemer op de hoogte gebracht van het bestaan van een eventuele onregelmatigheid en verwittigd van een mogelijke individualisering van de elektronische communicatiegegevens als er in de toekomst een nieuwe onregelmatigheid van dezelfde aard wordt vastgesteld. Pas dan kan worden overgegaan tot identificatie van de individuele werknemer(s) op basis van de andere gegevens die werden verzameld en zich op de server bevinden. Wanneer een individuele werknemer verantwoordelijk wordt geacht voor een (nieuwe) onregelmatigheid, moet hij worden uitgenodigd voor een gesprek waar hij het gebruik van de elektronische communicatiemiddelen kan rechtvaardigen.

2.3 Controle van de werknemers bij vermoeden van diefstal: cao nr. 89

Om diefstal in de onderneming te voorkomen, **mag de werkgever werknemers fouilleren, maar enkel bij het verlaten van de onderneming**. Volgens cao nr. 89 zijn dergelijke controles enkel toegelaten als ze gericht zijn op het voorkomen of vaststellen van de ontvreemding van goederen in de onderneming of op de werkplaats. Ze hebben niet tot doel de arbeidsprestaties van de werknemers te meten.

Systematische uitgangscontroles zijn alleen mogelijk als ze gebeuren door middel van elektronische en/of technische detectiesystemen. Uitgangscontroles uitgevoerd door personen mogen uitsluitend uitgevoerd worden door bewakingsagenten en niet door de werkgever.

Deze controles mogen enkel worden uitgevoerd:

- bij wijze van steekproef ter voorkoming van diefstal en in dat geval moet de controlemogelijkheid bestaan voor alle betrokken werknemers zonder onderscheid; of
- als er redelijke gronden zijn om te denken dat de werknemer goederen heeft ontvreemd, op basis van de gedragingen van de betrokkene, van materiële aanwijzingen of van de omstandigheden.

Voorafgaandelijk en bij het opstarten van een systeem van uitgangscontroles **moet de werkgever de OR over het systeem informatie verschaf-**

Privacy op de werkvloer en gegevensbescherming.indd 24 2/03/23 09:13

fen. Bij ontbreken van een OR wordt deze informatie verschaft aan het Comité PB, of bij ontbreken ervan aan de vakbondsafgevaardiging, of bij ontbreken ervan aan de werknemers.

Deze informatie heeft betrekking op:

- de perimeter van de onderneming of van de werkplaats ;
- de diefstalrisico's in de onderneming of op de werkplaats ;
- de maatregelen om die risico's te voorkomen of te verhelpen ; en
- de controlemethodes.

2.4 Geolocalisatie

Tot nu toe bestaat er **nog geen wetgeving over een probleem dat steeds vaker voorkomt in ondernemingen: «geolocalisatie».** De Gegevensbeschermingsautoriteit bracht hierover wel een advies uit (Advies nr. 12/2005 van 7 september 2005). Daarin stelt ze dat het toezicht op werknemers door middel van een monitoringsysteem verbonden met het GPS-navigatiesysteem van dienstwagens enkel toegelaten is mits naleving van het finaliteits-, proportionaliteits- en transparantiebeginsel , opnieuw de GDPR-beginselen dus.

Voor ondernemingen hun wagenpark uitrusten met een geolocalisatiesysteem, moeten ze een «geopolicy » opstellen die de beginselen en modaliteiten van een dergelijke controle bevat. Deze regels moeten worden vastgelegd in overleg met de vakbondsvertegenwoordigers in de overlegorganen van de onderneming. Het geolocalisatiebeleid moet onder meer de doeleinden en de frequentie van de controle nauwkeurig en expliciet vermelden en moet bij het arbeidsreglement worden gevoegd.

Een dergelijk systeem moet onder andere een « legitiem doeleinde» hebben om aanvaardbaar te zijn, nl.:

- de veiligheid van de werknemers verhogen tijdens werkgerelateerde verplaatsingen;
- de voertuigen van de ondernemingen en de vervoerde goederen beschermen;
- de vervoerstijd optimaliseren.

Privacy op de werkvloer en gegevensbescherming.indd 25 2/03/23 09:13

Controle van de prestaties van de werknemers kan ook worden beschouwd als een legitiem doeleinde, maar mag niet de enige reden zijn waarom de voertuigen worden uitgerust met een geolokalisatiesysteem. Een permanente controle waarbij er met behulp van een lokalisatiesysteem een systematische lezing van de geregistreerde gegevens plaatsvindt moet in principe als overmatig worden beschouwd. Tot slot is het verboden deze informatie te verzamelen buiten de werkuren wanneer de werknemer een dienstwagen gebruikt voor privédoeleinden na zijn dienst (om terug naar huis te rijden bv.). De werknemer zou het monitoringsysteem moeten kunnen deactiveren, wanneer hij niet werkt.

Volgens de GDPR mogen persoonsgegevens in principe enkel worden verwerkt met toestemming van de betrokkene of wanneer de verwerking nodig is om een overeenkomst uit te voeren waarbij de betrokkene partij is. Er bestaat nog een derde uitzondering op het verwerkingsverbod: het gerechtvaardigde belang van de onderneming.

De werkgever moet vooraf de volgende informatie meedelen :

- de rechtsgrondslag voor de gegevensverwerking (meestal het gerechtvaardigde belang van de onderneming) ;
- wie er wordt gecontroleerd;
- de doelstellingen die het geolokalisatiesysteem beoogt;
- de aard van de misbruiken die aanleiding kunnen geven tot controle;
- de duur van de controle;
- de verwerkte gegevens;
- of de gegevens aan landen buiten de Europese Unie worden doorgegeven;
- de rechten van de werknemer, met name het recht om de gegevens te raadplegen, het recht om een klacht in te dienen bij de Gegevensbeschermingsautoriteit, het recht om de gegevensverwerking te beperken ... ;
- de procedure die na de controle wordt gevolgd.

Volgens de Gegevensbeschermingsautoriteit moeten bepaalde systemen voor geolokalisatie in elk geval worden verboden, bv. om de naleving van de snelheidslimiet te controleren of om een werknemer permanent te controleren. Een dergelijk systeem kan met name niet worden gebruikt:

Privacy op de werkvloer en gegevensbescherming.indd 26 2/03/23 09:13

- in het voertuig van een werknemer die de vrijheid heeft zijn verplaatsingen zelf te regelen;
- om verplaatsingen van werknemersvertegenwoordigers in het kader van hun mandaat te volgen;
- om locatiegegevens op te halen buiten de werkuren (verplaatsingen van en naar het werk, pauzetijden, enz.), inclusief het tegengaan van diefstal of het controleren van de naleving van de gebruiksvoorwaarden van het voertuig;
- om de werktijd van werknemers te berekenen terwijl er al een ander systeem bestaat.

2.5 Cao nr. 38 betreffende de werving en selectie van werknemers

Tot slot vermelden we collectieve arbeidsovereenkomst nr. 38 waarin artikel 11 gaat over de eerbiediging van de persoonlijke levenssfeer van de sollicitanten. Daarin staat : *« De persoonlijke levenssfeer van de sollicitant zal bij de selectieprocedure worden geëerbiedigd. Dit impliceert dat vragen over het privéleven slechts verantwoord zijn indien zij relevant zijn voor de aard en de uitoefeningsvoorwaarden van de functie.»*

Privacy op de werkvloer en gegevensbescherming.indd 27 2/03/23 09:13

III. Privacy, gegevensbescherming en vakbondswerk

1. Persoonsgegevens en vakbondslidmaatschap

Vakbondslidmaatschap is een bijzondere categorie van persoonsgegevens: het is een gevoelig gegeven. Het is dus verboden dit soort gegeven te verwerken, behalve als de verwerking wordt verricht door *"een stichting, een vereniging of een andere instantie zonder winstoogmerk die op (...) vakbondsgebied werkzaam is, in het kader van haar gerechtvaardigde activiteiten en met passende waarborgen, mits de verwerking uitsluitend betrekking heeft op de leden of de voormalige leden van de instantie (...) en de persoonsgegevens niet zonder de toestemming van de betrokkenen buiten die instantie worden verstrekt"* (art. 9 GDPR). Ondernemingen en/of werkgevers kunnen in geen geval het vakbondslidmaatschap opvragen en verwerken.

Het ACV is de verwerkingsverantwoordelijke van de persoonsgegevens van zijn leden, en moet in die hoedanigheid alle verplichtingen voor een verwerkingsverantwoordelijke nakomen (zie boven), naast de beginselen wettigheid, rechtmatigheid, evenredigheid en transparantie. Meer info daarover vind je op onze website en in onze folder « Hoe gaat het ACV om met je persoonsgegevens?".

2. Gebruik van persoonsgegevens door vakbondsvertegenwoordigers

Het ACV is dus de verwerkingsverantwoordelijke van zijn leden. Maar als vakbondsvertegenwoordiger kom je wellicht regelmatig terecht in situaties waar persoonsgegevens meespelen, al was het maar om met je collega's te communiceren over een actueel thema in je onderneming. Welke regels moet je dan volgen?

Communicatie met leden

Het verzenden van vakbondsinformatie en propaganda naar onze leden is geen probleem omdat het gebaseerd is het gerechtvaardigd belang van het ACV.

Tenzij anders vermeld, mag je de leden mails sturen met syndicale berichten. Let wel op, want een lid kan aangeven dat het geen mails meer van ons wenst te ontvangen.

Privacy op de werkvloer en gegevensbescherming.indd 29 2/03/23 09:13

Eventueel kunnen lijsten worden opgesteld van wie al dan niet berichten van ons wil ontvangen.

TIP: gebruik de BCC-optie bij het verzenden van een mail naar meerdere personen. De e-mailadressen van je ontvangers zijn dan niet zichtbaar.

Communicatie met niet-leden

Als je vakbondsinformatie wil bezorgen aan collega's die geen ACV-lid zijn, moet je voorzichtig zijn. Zij moeten altijd kunnen aangeven dat ze geen vakbondsinformatie meer willen ontvangen. Nogmaals: er moet dus een praktische oplossing voor handen zijn om de wens van de werknemers na te komen.

Tot slot is een ander belangrijk element dat de informatie altijd via de vakbondsvertegenwoordiger(s) in de onderneming moet worden verpreid en niet afkomstig mag zijn van de vakbondsorganisatie zelf.

Krachtens cao nr. 5 zal "de syndicale afvaardiging mondeling of schriftelijk kunnen overgaan tot alle mededelingen welke nuttig zijn voor het personeel [...]."

Een afgevaardigde kan dus nooit worden aangerekend dat hij e-mails met syndicale inlichtingen naar alle personeelsleden stuurt.

Anderzijds heeft de werkgever geen wettelijke verplichting om de lijst met de namen van de personeelsleden aan de VA te bezorgen, maar als de VA een dergelijke lijst (die hij eventueel zelf heeft samengesteld, bijvoorbeeld via het Outlook-adresboek) zou gebruiken om via mail met het personeel te communiceren, kan de werkgever of de DPO hem dat niet aanrekenen.

3. Impact van de GDPR op het sociaal overleg

Als je vakbondsafgevaardigde bent of zetelt in een sociaal overlegorgaan, heb je het misschien al meegemaakt dat de werkgever jullie "op

Privacy op de werkvloer en gegevensbescherming.indd 30 2/03/23 09:13

grond van de GDPR" geen informatie meer geeft. De GDPR mag dan wel voor iedereen een belangrijke bescherming bieden wat onze persoonlijke gegevens betreft, de verordening mag niet worden misbruikt om de sociale overlegorganen te omzeilen!

Voor alle duidelijkheid: de GDPR heeft geen impact op de gegevens die aan de vakbondsvertegenwoordigers in de overlegorganen worden meegedeeld. De meeste van de meegedeelde gegevens zijn inderdaad niet-nominatief, dat wil zeggen dat ze geanonimiseerd of gebundeld werden, waardoor de betrokkenen niet kunnen worden geïdentificeerd. Het gaat dus eenvoudigweg niet om persoonlijke gegevens, omdat je de gegevens niet kan linken aan een bepaalde persoon. De GDPR-verplichtingen zijn dus niet van toepassing.

Cao nr. 9 zegt ons dat : « *het ondernemingshoofd of zijn afgevaardigde aan de ondernemingsraad de gegevens (zal) verstrekken die deze laatste moeten toelaten zich een duidelijk beeld te vormen over de structuur van de tewerkstelling in de onderneming, over haar evolutie en over de vooruitzichten inzake tewerkstelling* ». De gegevens zijn niet-nominatief. Er is sprake van "personeel". Er worden geen namen maar wel cijfers genoemd. Het zijn dus geen persoonsgegevens. Een onderneming mag de GDPR niet gebruiken als argument om dit soort gegevens niet te verstrekken.

Nominatieve gegevens zijn daarentegen wel persoonsgegevens. De toestemming van de betrokkenen is noodzakelijk, behalve als de verwerking van deze gegevens een wettelijke verplichting is. Bijvoorbeeld met betrekking tot het onthaal van nieuwe werknemers. **De werkgever moet hun naam aan de vakbondsvertegenwoordigers meedelen zodat zij hun onthaal kunnen organiseren** (cao nr. 22). De verwerkingsverantwoordelijke is de werkgever, die deze gegevens verzamelt om ze aan de vakbondsvertegenwoordigers te bezorgen. Het is aan hem om de privacy van zijn werknemers tijdens deze verwerking te respecteren.

Op dezelfde manier is **de vakbondsafvaardiging, in het kader van haar syndicale taken, verantwoordelijk voor het toezicht op de naleving van de sociale wetgeving door de werkgever** (cao nr. 5). In dat kader heeft ze bijvoorbeeld **het wettelijke mandaat om toezicht te houden op de naleving van de regels aangaande overuren** (arbeidswet). Daartoe moet de werkgever de nodige informatie verstrekken over de personen die overuren hebben gepresteerd en wanneer. Erg vaak beschouwt de werkgever dit echter als persoonlijke gegevens en weigert hij die te verspreiden. **Nochtans hebben de leden van de vakbondsafvaardiging discretie-**

Privacy op de werkvloer en gegevensbescherming.indd 31 2/03/23 09:13

plicht ten opzichte van die informatie. Het is duidelijk dat de werkgever op die manier het toezicht op de toepassing van de wetgeving door de vakbondsafvaardiging in de weg staat.

Een belangrijk argument om in het achterhoofd te houden wanneer een werkgever weigert informatie te geven terwijl hij daartoe wel verplicht is (omdat de wet of een cao erin voorziet) is artikel 88 van de GDPR.

Volgens dit artikel "kunnen de lidstaten nadere regels vaststellen ter bescherming van de rechten en vrijheden met betrekking tot de verwerking van de persoonsgegevens van werknemers in het kader van de arbeidsverhouding" (art. 88 GDPR). Dit kunnen nationale wetten of nationale, sectorale of ondernemingscao's zijn. De GDPR erkent via dit artikel de rechtsgeldigheid van al deze wetgeving, als rechtsgrond voor de verwerking van persoonsgegevens. Dat betekent dat elke wet of cao die het mogelijk maakt of vereist dat gegevens worden verwerkt, moet worden gerespecteerd, ondanks de GDPR. In dit artikel bevestigt de GDPR eigenlijk dat alle nationale wetten uitzonderingen kunnen zijn op het verbod op de verwerking van persoonsgegevens. Want zoals we hebben gezien, is een van de voorwaarden voor het verwerken van gegevens het naleven van een wettelijke verplichting.

Als de onderneming op basis van een wettelijke bepaling verplicht is om bepaalde informatie aan de overlegorganen te verstrekken, kan ze zich dus niet verschuilen achter de GDPR en moet ze die respecteren en de informatie geven. Omgekeerd: als een Belgische wet verder gaat dan de GDPR op het vlak van gegevensbescherming, moet ze ook gerespecteerd worden.

Kortom, de Europese verordening verandert niets fundamenteels aan het recht op informatie van de leden van de verschillende sociale overlegorganen. Alle nationale, sectorale en ondernemingscao's blijven van toepassing. De rechtsgronden voor informatie-raadpleging en voor de bevoegdheden van de leden van de OR, het Comité PB en de VA blijven van toepassing en de gewoonlijk verkregen informatie moet ook in de toekomst verder worden verstrekt.

Wat wel zou kunnen, is dat men werknemersvertegenwoordigers vertrouwelijkheidsclausules laat ondertekenen die verzekeren dat ze die gegevens alleen in het kader van hun mandaat gebruiken.

Privacy op de werkvloer en gegevensbescherming.indd 32 2/03/23 09:13

Bijzonder geval: sociale verkiezingen

Krachtens de wet van 4/12/2007 betreffende de sociale verkiezingen worden een aantal persoonsgegevens verwerkt door de vakbondsvertegenwoordigers, zoals de lijst van het leidinggevend personeel en van de werknemers die een kaderfunctie uitoefenen, de kandidatenlijst, de samenstelling van de stembureaus en de getuigenlijsten.

De kiezerslijsten, die door de werkgever worden opgesteld, worden in de ondernemingsraad of het Comité PB goedgekeurd en vervolgens ter beschikking gesteld van alle werknemers, met het oog op transparantie en collectieve controle tijdens de volledige kiesprocedure in de onderneming, en waardoor elke werknemer eventueel een klacht kan indienen in geval van vergissing. Let wel: de kiezerslijst mag niet worden verward met de lijst van de personeelsleden. De wetgeving m.b.t. de sociale verkiezingen verplicht enkel dat de eerste lijst moet worden verzonden, de tweede niet. In beginsel dient de werkgever de ondernemingsraad en/of het Comité PB dus enkel de gegevens te bezorgen die nodig zijn om deze kiezerslijsten op te stellen.

4 Controleren of de werkgever de GDPR respecteert

Als vakbondsvertegenwoordiger zal een nieuw onderdeel van je vakbondswerk erin bestaan te **verzekeren dat de werkgever voldoet aan de GDPR-verplichtingen** en dat hij niet zomaar om het even welke gegevens verwerkt. Eerst moet je nagaan of de werkgever transparant is: de werkgever heeft de plicht om zijn werknemers te informeren over de verwerkte gegevens. Om deze transparantieplicht na te leven, is het mogelijk dat de werkgever een beleid voor gegevensverwerking opstelt. Het uitwerken van een ondernemingscao is ook een mogelijkheid, wat de voorkeur geniet uit syndicaal oogpunt, zodat de vakbondsafgevaardigden betrokken worden bij de afsluiting van die cao.

Privacy op de werkvloer en gegevensbescherming.indd 33 2/03/23 09:13

Om te zien of de werkgever de rechten van werknemers en zijn nieuwe verplichtingen als werkgever en verwerkingsverantwoordelijke respecteert, kan het ten slotte **nuttig zijn erop toe te zien dat het arbeidsreglement up-to-date is**, als de GDPR wijzigingen in het arbeidsreglement meebrengt.

Deze lijst geeft enkele vragen weer die nuttig kunnen zijn als werknemervertegenwoordiger:

- Welke persoonsgegevens wil de werkgever verwerken?
- Gaat het om gevoelige persoonsgegevens?
- Bestaat er een rechtsgrondslag (doel) voor de verwerking?
- Worden de basisprincipes voor verwerking nageleefd? (met name minimalisering.
- Heeft de werkgever de gepaste (technische/operationele) veiligheidsmaatregelen genomen?
- Kennen de betrokkenen (de werknemers) hun rechten?
- Worden die rechten correct nageleefd (gegarandeerd)?

V.U. : D. Leyon, Haachtsesteenweg 579 - 1030 Brussel - www.acv-online.be - D/2023/0780/1

facebook.com/het.acv

@ACV_Vakbond

ACVvakbond

acv.vakbond