PARTENA PROFESSIONAL

# MEMENTO

## VAN DE WERKGEVER 06

Maandelijks informatieblad over sociale en fiscale reglementering | Partena Professional | Juni 2018

# DOSSIER

## Privacy op de werkvloer (deel II)


A. WAAR BEGINNEN? DRIE CRUCIALE STAPPEN >
B. DE RECHTSGROND VAN DE VERWERKING >
C. GEVOELIGE PERSOONSGEGEVENS >
D. STRAFRECHTELIJKE PERSOONSGEGEVENS >
E. FORMALITEITEN >
F. HOE LANG PERSOONSGEGEVENS BIJHOUDEN? >
G. DOORGIFTE AAN LANDEN BUITEN DE EU >
H. DE DATA PROTECTION OFFICER: NIET ALTIJD VERPLICHT >
I. TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMAATREGELEN >
J. MELDINGSPLICHT >
K. SANCTIES >
L. U KUNT NU AAN DE SLAG >


# ACTUALITEIT


## Starterslonen: uitstel

## Bedrijfssmartphone en split bill: de fiscus verduidelijkt



## COLOFON

Partena – vereniging zonder winstoogmerk – sociaal secretariaat van werkgevers erkend door MB van 3 maart 1949 met nr. 300
Maatschappelijke zetel: Kartuizersstraat 45, 1000 Brussel, btw BE 0409.536.968.

Verantwoordelijke uitgever: Alexandre Cleven.
Ere-hoofdredacteur: Francis Verbrugge.
Hoofdredacteur: Yves Stox, yves.stox@partena.be

Verschijnt niet in juli en augustus. De overname van teksten, zelfs gedeeltelijk, is slechts toegestaan na schriftelijke toestemming van de redactie en mits de bron wordt vermeld.
De redactie streeft naar betrouwbaarheid van de gepubliceerde informatie, maar kan niet aansprakelijk worden gesteld voor de juistheid ervan.

40e jaar – maandblad


PARTENA PROFESSIONAL

DOSSIER PRIVACY OP DE WERKVLOER (DEEL II)

# DE NIEUWE REGELS VAN DE ALGEMENE VERORDENING GEGEVENSBESCHERMING GDPR

In het meinummer kunt u het eerste deel terugvinden over de Algemene Verordening Gegevensbescherming (Verordening 2016/679 van 17 april 2016). De Algemene Verordening Gegevensbescherming is beter bekend als het acroniem GDPR en is van toepassing sinds 25 mei 2018. In dit tweede deel bekijken we met name hoe u aan de slag kunt voor de praktische uitwerking van de GDPR.

## A. WAAR BEGINNEN? DRIE CRUCIALE STAPPEN[1]

Bij de implementatie van de GDPR zijn drie stappen cruciaal.

1) Breng in kaart welke persoonsgegeven u bijhoudt. Waar komen ze vandaag en met wie deelt u deze persoonsgegevens?
2) Analyseer welke types van gegevenswerking plaatsvinden.
3) Identificeer de rechtsgrond voor elk type van gegevensverwerking.

De reden is tweeledig.

- U moet als werkgever-verwerkingsverantwoordelijke altijd over een juridische basis beschikking om persoonsgegevens te mogen verwerken.
- Sommige persoonsgegevens zijn gevoelig. Het is in principe verboden om die te verwerken.

Deze twee elementen werken we hieronder verder uit.

## B. DE RECHTSGROND VAN DE VERWERKING

U moet als werkgever-verwerkingsverantwoordelijke altijd over een juridische basis beschikking om persoonsgegevens te mogen verwerken:

1) de toestemming;
2) de uitvoering van een overeenkomst;
3) een wettelijke verplichting; of
4) gerechtvaardigde belangen.

U hebt dus niet altijd de toestemming nodig van de individuele betrokkene. Dat geldt enkel voor de gevoelige persoonsgegevens. Eén rechtsgrond is voldoende om de persoonsgegevens te mogen verwerken. Niets belet u om toch steeds toestemming te vragen, ook al beschikt u over een andere rechtsgrond. Die afweging moet u maken. Door steeds de toestemming te vragen speelt u op veilig. Maar hou er rekening mee dat niet elke werknemer zonder meer zal toestemmen. Zal u dan de verwerking toch doorvoeren op basis van bijvoorbeeld de uitvoering van de overeenkomst, ook al beschikt u niet over de toestemming van de werknemer?

### 1. DE TOESTEMMING

U mag de persoonsgegevens verwerken indien de betrokken, werknemer of sollicitant, zijn of haar toestemming heeft gegeven voor de verwerking.[2] Die toestemming moet wel aan vier cumulatieve voorwaarden voldoen:[3] U draagt als werkgever-verwerkingsverantwoordelijke de bewijslast dat de betrokkene toestemt met de verwerking.[4]

1) **De betrokkene moet geïnformeerd zijn**
   De werknemer of sollicitant moet weten waarvoor hij of zij toestemming verleent. De GDPR bepaalt niet op welke manier u de betrokkene moet informeren. U moet de betrokkene hebben geïnformeerd voordat u de toestemming verkrijgt.

2) **De toestemming moet vrij zijn**
   In de context van de arbeidsverhouding rijst de vraag of een werknemer wel vrij zijn toestemming kan geven. Verhindert het werkgeversgezag de vrije toestemming van de werknemer? De toestemming van een werknemer aan zijn of haar werkgever in het kader van de GDPR kan vrij zijn.[5]

U mag de toestemming in ieder geval niet afdwingen. De werknemer moet overigens op elk moment zijn of haar toestemming kunnen intrekken.[6] De intrekking heeft enkel uitwerking voor de toekomst. "Vrij" betekent dat het al dan niet instemmen of intrekken niet mag worden gesanctioneerd. Dat betekent dat u in bepaalde omstandigheden een alternatieve werkplek of arbeidsomstandigheden moet voorzien voor de werknemer die weigert om toe te stemmen met de verwerking.

België kan specifieke regels vastleggen voor de voorwaarden waaronder persoonsgegevens in de context van een arbeidsverhouding mogen worden verwerkt op basis van de toestemming. Vóór de inwerkingtreding van de GDPR bepaalde de Belgische privacyregelgeving dat een sollicitant of werknemer in de regel niet vrij zijn of haar toestemming kan geven. Dit verbod gold niet wanneer de verwerking erop gericht was de betrokkene een voordeel te verstrekken.[7] Het is niet duidelijk of deze regel zal worden hernomen in de toekomst.

Voor de verwerking van heel wat persoonsgegevens is de toestemming van de betrokkene geen vereiste om de eenvoudige reden dat u één van de andere rechtsgronden kunt hanteren. Dat is niet zo voor gevoelige persoonsgegevens. Om persoonlijke gegevens te verwerking is toestemming in de regel vereist.

#### 3) De toestemming moet specifiek zijn

Dat betekent dat u het verzoek om toestemming niet zomaar verwerkt als onderdeel van een tekst die ook andere elementen bevat. U moet het verzoek om toestemming in een begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal formuleren.

U moet de tekst zo vormgeven dat de betrokkene het verzoek om toestemming duidelijk kan onderscheiden van de andere aangelegenheden.[8]

#### 4) De toestemming moet ondubbelzinnig zijn

De werknemer of sollicitant geeft de toestemming door een expliciete verklaring of een ondubbelzinnige en actieve handeling. Dat kan een ondertekende verklaring zijn, al is dat niet de enige manier om een toestemming te verkrijgen. Het invullen van een formulier online of het sturen van een e-mail worden ook aanvaard. Een selectievakje of aankruisvakje dat al is aangevinkt voldoet dan weer niet.

## 2. DE UITVOERING VAN EEN OVEREENKOMST

De verwerking is ook rechtmatig als die verwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene een partij is. De verwerking is eveneens rechtmatig als de betrokkene voorafgaand aan het afsluiten van de overeenkomst vraagt om maatregelen te nemen (zie het meinummer).[9] In de praktijk geeft deze rechtsgrond een ruime rechtsgrond voor de meeste vormen van gegevensverwerking van werknemers. Toch is deze rechtsgrond geen vrijbrief voor elke vorm van gegevensverwerking. De verwerking moet noodzakelijk zijn voor de uitvoering van de overeenkomst.

**VOORBEELD 1**

**U moet de werknemer geen toestemming vragen voor de verwerking van zijn of haar gegevens in de loonadministratie. Die is namelijk noodzakelijk voor de correcte uitvoering van de arbeidsovereenkomst.**

**VOORBEELD 2**

U kunt de verwerking van persoonsgegevens via een evaluatie- en opleidingssoftware op deze rechtsgrond steunen, zonder dat u de individuele toestemming van de werknemer moet verkrijgen. De uitvoering van de arbeidsovereenkomst wordt onmogelijk indien u niet over de mogelijkheden beschikt om te waken over de sterktes en zwaktes van een individuele werknemers en de opleidingskansen daarop af te stemmen.

### 3. EEN WETTELIJKE VERPLICHTING

De verwerking van persoonsgegevens kunt u ook rechtvaardigen op basis van een wettelijke verplichting. U moet de persoonsgegevens verwerken omdat de regelgeving u dat nu eenmaal oplegt.[10]

**VOORBEELD**

U moet familiale gegevens van een werknemers verwerken en doorgeven aan de fiscus in het kader van de loonadministratie. U kunt deze verwerking dus verrichten zonder de toestemming van de werknemer.

### 4. GERECHTVAARDIGDE BELANGEN

Dit is wellicht de meest complexe manier om de verwerking van persoonsgegevens te rechtvaardigen. U mag persoonsgegevens verwerken als ze noodzakelijk zijn voor de behartiging van uw gerechtvaardigde belangen als verwerkingsverantwoordelijke of de belangen van een derde.[11] Dat betekent dat u de belangen van de werknemers moet afwegen ten opzichte van uw eigen belang als verwerkingsverantwoordelijke. Dat is moeilijk en de uitkomst is onzeker.

**VOORBEELD**

U kunt overwegen om de verwerking van persoonsgegevens in het kader van een klokkenluidersregeling op deze rechtsgrond te baseren. Via zo een intern meldingssysteem kunnen werknemers hun vermoedens of informatie in verband met fraude en corruptie melden.[12]

## C. GEVOELIGE PERSOONSGEGEVENS

Gevoelige persoonsgegevens mag u in principe niet verwerken.[13]
Het gaat dan om:

- de persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken,
- genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon
- gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

**VOORBEELD**

De verwerking van foto's mag niet systematisch worden beschouwd als verwerking van gevoelige persoonsgegevens. Foto's kunnen wel onder de definitie van biometrische gegevens vallen wanneer de verwerking de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maakt.[14]
Foto's opnemen op het intranet in een who-is-who kan dus, ook zonder de toestemming van de individuele werknemer. Als onderneming hebt u een gerechtvaardigd belang om een fotoboek bij te houden. Het helpt om het intern communicatieproces vlot te laten lopen.[15]

Toch zijn er een aantal uitzonderingen op het principiële verbod om gevoelige persoonsgegevens te verwerken.[16]

1) De betrokkene heeft uitdrukkelijke toestemming gegeven voor de verwerking. (België kan wel bepalen wanneer die individuele toestemming niet kan worden ingeroepen.)
2) De verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van uw rechten als werkgever-verwerkingsverantwoordelijke of de betrokkene op het gebied van het arbeidsrecht en de sociale zekerheid.
3) De verwerking heeft betrekking op persoonsgegevens die duidelijk door de betrokkene openbaar zijn gemaakt.
4) De verwerking is noodzakelijk voor een rechtsvordering (instelling, uitoefening of onderbouwing).
5) De verwerking is noodzakelijk voor doeleinden van preventieve of arbeidsgeneeskunde.

De lidstaten kunnen bovendien voorwaarden en beperkingen invoeren met betrekking tot de verwerking van genetische gegevens, biometrische gegevens of gegevens over gezondheid.

## D. STRAFRECHTELIJKE PERSOONSGEGEVENS

Voor persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten gelden bijzondere voorwaarden. Zelfs met de toestemming van de sollicitant of werknemer kunt u die alleen verwerken indien de wetgeving die verwerking toestaat.[17] U mag dus een 'uittreksel strafregister' (vervangt het 'bewijs van goed zedelijk gedrag') verwerken voor functies waar de wet of toezichthouder dat vereist, zoals voor bedrijfsrevisoren, boekhoudkundige en fiscale beroepen, de opvoeding van minderjarigen. Dat 'uittreksel strafregister' bevat niet alle veroordelingen, maar de veroordelingen die relevant zijn voor de functie.[18]

Mag u tijdens de sollicitatieprocedure vragen om een 'uittreksel strafregister' voor te leggen? De GDPR verbiedt de verwerking van strafrechtelijke gegevens. Maar wat indien u een kandidaat vraagt om het bewijs van goed gedrag en zeden voor te leggen, het leest, en het vervolgens hem of haar opnieuw bezorgt? De vroegere privacycommissie was van oordeel dat u op die manier geen strafrechtelijke gegevens hebt verwerkt.[19]

## E. FORMALITEITEN

U hebt in kaart gebracht welke persoonsgegevens u bijhoudt, geanalyseerd welke gegevensverwerking plaatsvind binnen uw onderneming en

per verwerking de rechtsgrond geïdentificeerd. Die stappen moet u doorlopen om uiteindelijk te bepalen welke formaliteiten u moet vervullen.

**VOORBEELD 1**

U hebt geïdentificeerd dat u in de personeel- en loonadministratie identificatiegegevens van werknemers verwerkt. U deelt die gegevens ook met uw sociaal secretariaat. U doet dat om de uitvoering van de arbeidsovereenkomst mogelijk te maken en om te voldoen aan de wettelijke verplichtingen in het kader van de arbeidsrelatie.

**VOORBEELD 2**

U ziet nauw toe op wie toegang heeft tot de R&D-afdeling binnen uw onderneming. Werknemers hebben toegang tot de arbeidsplek na biometrische authenticatie, bijvoorbeeld door een vingerafdruk. Dat zijn gevoelige persoonsgegevens. U heb de toestemming van elke individuele werknemer nodig.

Afhankelijk van de concrete situatie moet u verschillende formaliteiten vervullen in het kader van de arbeidsrelatie:

1) De opmaak van een register van de verwerkingsactiviteiten;
2) De opmaak van een privacy policy;
3) Het aanpassen van het arbeidsreglement is niet verplicht en zelden aan te raden, maar het afsluiten van een bijlage bij de arbeidsovereenkomst kan wel een oplossing bieden.

Elk van deze documenten lichten we hieronder verder toe.

### 1) Het register van de verwerkingsactiviteiten

Vóór 25 mei 2018 moest u alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens aangeven bij de vroegere privacycommissie. Het register van de verwerkingsactiviteiten vervangt die aanmeldingsverplichting.[20]

#### a. Een verplichting voor werkgevers

Als werkgever-verwerkingsverantwoordelijke moet u het register van de verwerkingsactiviteiten opmaken en bijhouden.[21] Dat register documenteert alle verwerkingsactiviteiten die onder u verantwoordelijkheid gebeuren.

Niet elke verwerkingsverantwoordelijke is verplicht om een register van de verwerkingsactiviteiten op te maken. Deze verplichting geldt niet voor ondernemingen die minder dan 250 personen in dienst hebben.[22]
Deze uitzondering is theoretisch. In de praktijk moet een werkgever met minder dan 250 werknemers een register opmaken. Ook een kleine onderneming met minder dan 250 werknemers moet namelijk een register opmaken indien de verwerking niet-incidenteel is. Personeelsbeheer is eigenlijk nooit incidenteel.[23]

U moet het register schriftelijk en elektronisch bijhouden.[24] U moet het niet publiek maken, voorleggen aan de werknemers(vertegenwoordigers) of toesturen aan de GBA (Belgische Gegevensbeschermingsautoriteit).

Het register is een controle-instrument. De GBA kan u vragen om het register voor te leggen en dan moet u het onmiddellijk bezorgen aan deze toezichthouder. [25]

Het is een dynamisch document. U moet u het steeds aanpassen aan de hand van de reële verwerking van persoonsgegevens binnen uw onderneming.

U moet het register opmaken en bijhouden voor alle verwerkingen van persoonsgegevens. Niet alleen voor de verwerkingen in het kader van de arbeidsrelatie. Verwerkt u ook de persoonsgegevens van bijvoorbeeld klanten? Dan moet u die verwerkingen ook opnemen in het register van de verwerkingsactiviteiten.

**b. Welke gegevens opnemen in het register?**

Het register van de verwerkingsactiviteiten moet de volgende gegevens bevatten:[26]

- de naam en de contactgegevens van de (gezamenlijke) verwerkingsverantwoordelijke(n), de vertegenwoordiger en de functionaris voor gegevensbescherming (indien van toepassing);
- 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;[27]
- doorgifte van persoonsgegevens aan een derde land of een internationale organisatie (indien van toepassing);
- indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

U herkent zeker en vast een aantal gegevens die u ook aan de werknemers moet bezorgen in het kader van uw informatieplicht. U moet de werknemers informeren, maar u moet dat niet doen aan de hand van het register. Een privacy policy is een instrument dat u hierbij kan helpen. Vraagt u de werknemers hun akkoord voor de werking door middel van een bijlage aan de arbeidsovereenkomst? Dan kunt u hen ook via die weg informeren.

**c. Een voorbeeld**

De GDPR legt geen specifieke template op. U bepaalt dus zelf hoe het register van de verwerkingsactiviteiten eruitziet.
Hieronder kunt u een voorbeeld vinden. We hebben het ingevuld aan de hand van twee voorbeelden die u hoger terugvindt:

1) De verwerking van identificatiegegevens in de personeel- en loonadministratie;
2) Biometrische toegangscontrole tot de afdeling R&D.

| Verwerkings-gegevens / categorieën van gegevens | Doeleinden | Betrokkenen | Rechtsgrond | Ontvangers | Ontvangers derde landen | Bewaringstermijn |
|---|---|---|---|---|---|---|
| **A. Identificatiegegevens** | | | | | | |
| identificatiegegevens: naam, titel, adres (privé, werk), vroegere adressen | personeels- en loonadministratie; evaluatie van het personeel; werkplanning; toegangscontrole; controle op de werkvloer | personeelsleden in dienst van de werkgever; personen werkzaam ten behoeve van de werkgever | uitvoering arbeidsovereenkomst werkgever en werknemer; voldoen aan de wettelijke verplichtingen in het kader van een arbeidsrelatie. Noodzakelijke goede werking van de onderneming | werkgever en professionele raadgevers van de werkgever; personeelsleden van de werkgever belast met de personeelsadministratie | neen | 5 jaar na einde van de arbeidsovereenkomst |
| **B. Financiële gegevens** | | | | | | |
| financiële identificatiegegevens: identificatie– en bankrekeningnummers. | personeels-en loonadministratie | personeelsleden in dienst van de werkgever; personen werkzaam ten behoeve van de werkgever | uitvoering arbeidsovereenkomst werkgever en werknemer; voldoen aan de wettelijke verplichtingen in het kader van een arbeidsrelatie | werkgever en professionele raadgevers van de werkgever; personeelsleden van de werkgever belast met de personeelsadministratie | neen | 5 jaar na einde van de arbeidsovereenkomst |
| **C. Fysieke gegevens** | | | | | | |
| fysieke gegevens: onderscheidende kenmerken | biometrische identificatie | personeelsleden in dienst van de werkgever bij de afdeling R&D | Individuele toestemming van de betrokkene | werkgever; firma gespecialiseerd in toegangscontrole; personeelsleden van de werkgever belast met de personeelsadministratie | neen | 12 maand na einde van de arbeidsovereenkomst |

### 2) De opmaak van een privacy policy

De GDPR verplicht u om informatie te verstrekken wanneer u persoonsgegevens verwerkt die u ofwel direct via de betrokkene heeft bekomen[28] of die u via een derde heeft bekomen. Een privacy policy is een manier om aan deze verplichting te voldoen.

Heel wat informatie uit het register van de verwerkingsactiviteiten zal zijn plaats vinden in de privacy policy. In de privacy policy geeft u een antwoord op de vragen die u moet beantwoorden om te voldoen aan de informatieverplichting (zie het eerste deel in het meinummer).

Wie is de verwerkingsverantwoordelijke? Wat zijn de doeleinden van de verwerking? Wat is de rechtsgrond van de verwerking? Wie ontvangt de persoonsgegevens? Geeft u de persoonsgegevens door buiten de Europese Unie? Wat is de bewaartijd van de persoonsgegevens? Is de verstrekking van persoonsgegevens een verplichting of een voorwaarde? Wat zijn de betrokken categorieën van persoonsgegevens?

De GDPR verplicht u ook om de betrokkene te informeren over hun rechten. Ook die informatie neemt u op in de privacy policy.
Het recht van inzage en kopie, het recht op rectificatie, het recht op uitwissing van de gegevens, het recht op beperking van de verwerking, het recht van bezwaar en geautomatiseerde individuele besluitvorming, het recht op overdraagbaarheid, het recht om een klacht in te dienen bij de GBA.

De privacy policy is een dynamisch document, net als het register van de verwerkingsactiviteiten. U moet beide documenten aanpassen aan de hand van de reële verwerking van persoonsgegevens binnen uw onderneming. Herinner de lezer van de privacy policy er dan ook aan dat u het document in de toekomst zal aanpassen. De GDPR legt daarvoor geen specifieke procedure op. Informeer de betrokkenen van de aanpassing.

### 3) Het arbeidsreglement en de bijlage bij de arbeidsovereenkomst

U kunt in theorie de werknemers informeren via het arbeidsreglement. Daar zijn twee belangrijke nadelen aan verbonden.

1) Het arbeidsreglement is enkel van toepassing op werknemers en bijvoorbeeld leerlingen 'alternerend leren'. De impact van de GDPR is ruimer dan alleen werknemers, ook in de context van de arbeidsrelatie. Wanneer u dus de gegevens van sollicitanten verwerkt, moet u die informeren via een apart kanaal. Een privacy policy garandeert een meer globale aanpak en is wellicht ook praktischer.
2) Het arbeidsreglement is geen dynamisch instrument. U moet een strikte procedure toepassen wanneer u het wilt wijzigen.[29] De looptijd van die procedure maakt dat u in de praktijk niet steeds voldoet aan de informatieplicht die de GDPR u oplegt.

U kunt de werknemers informeren door middel van de bijlage bij de arbeidsovereenkomst.

1) Dat zal nuttig zijn indien u sowieso de toestemming van de werknemer nodig heeft of wenst voor het verwerken van de persoonsgegevens. Alles in één document, dat is makkelijk om te implementeren.
2) Ook de bijlage bij de arbeidsovereenkomst mist het dynamische karakter dat de GDPR vraagt. Dat zal u vooral parten spelen indien de gegevensstromen binnen uw onderneming snel en sterk kunnen

wijzigen. Om dit te verhelpen kunt u natuurlijk de bijlage bij de arbeidsovereenkomst combineren met een privacy policy.

## F. HOE LANG PERSOONSGEGEVENS BIJHOUDEN?

De Belgische wetgeving verplicht u om het (speciale) personeelsregister[30], de individuele rekening en de eventuele bijlagen (kopies van loonstaten enz.) gedurende vijf jaar te bewaren. Dat zijn heel precieze regels.

- Zo begint voor het (speciale) personeelsregister de bewaartermijn te lopen de zevende dag na de datum van uitdiensttreding van de laatste werknemer.
- Voor de individuele rekening (en de eventuele bijlagen), start de bewaartermijn vanaf de jaarlijkse afsluiting van de rekening. Maar ontstaat er een betwisting over een betaling na het vertrek van de werknemer, dan moet u het document bewaren tot vijf jaar na datum waarop de laatst vermelde sommen moeten aangegeven zijn bij de RSZ.

Deze termijnen zijn minimumtermijnen. De Belgische wetgeving legt geen maximumtermijnen op. Welke regel moet u dan hanteren? U kunt niet anders dan terugvallen op het algemene principe van de GDPR. U mag persoonsgegevens niet langer bewaren dan nodig is voor de verwezenlijking van de doelen waarvoor deze gegevens worden verzameld en gebruikt.

- In het register van de verwerkingsactiviteiten kozen wij voor vijf jaar. Dat betekent dat u de identificatiegegevens in de personeel- en loonadministratie even lang bijhoudt als de individuele rekening zelf.
- Voor de biometrische toegangscontrole kozen wij in het register van de verwerkingsactiviteiten voor 12 maanden. Deze termijn is in lijn met de verjaringstermijn van rechtsvorderingen die uit de arbeidsovereenkomst ontstaan.[31]

Bepaal daarom steeds de bewaringstermijn in functie van de doelstelling die u wilt bereiken binnen uw onderneming met het bewaren van de betrokken persoonsgegevens.

## G. DOORGIFTE AAN LANDEN BUITEN DE EU[32]

Binnen de Europese Unie kunnen persoonsgegevens vrij circuleren. Voor landen buiten de EU moet u als verwerkingsverantwoordelijke zich vergewissen dat een passende bescherming wordt gewaarborgd. Dat betekent dat de privacywetgeving van het betrokkenland een beschermingsniveau biedt dat vergelijkbaar is met de GDPR.

Voor sommige landen moet u geen bijkomende maatregelen nemen. Dat is bijvoorbeeld het geval voor de Verenigde Staten, op voorwaarde dat de betrokken onderneming aangesloten is bij de EU-US Privacy Shield (het vroegere Safe Harbour).

Biedt het andere land geen passend bescherming? Dan moet u privacybescherming waarborgen aan de hand van bindende bedrijfsvoorschriften (binnen een groep van ondernemingen) of door standaardbepalingen inzake gegevensbescherming op te nemen in uw overeenkomst met bijvoorbeeld de betrokken onderaannemers of dienstverleners.

## H. DE DATA PROTECTION OFFICER NIET ALTIJD VERPLICHT

De GDPR verplicht sommige ondernemingen om een data protection officer (dpo of functionaris voor de gegevensbescherming) aan te stellen. De kans is groot dat u niet bent verplicht om een dpo aan te stellen. Die verplichting geldt enkel voor:

- een overheidsinstantie of overheidsorgaan;
- de onderneming hoofdzakelijk belast met verwerkingen die vanwege hun aard, hun omvang en/of hun doeleinden regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen;
- de onderneming hoofdzakelijk belast met grootschalige verwerking van gevoelige persoonsgegevens en strafrechtelijke persoonsgegevens.[33]

## I. TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMAATREGELEN

De GDPR legt op om een risicoanalyse of gegevensbeschermingseffectbeoordeling (privacy impact assessment of PIA) uit te voeren. Die risicoanalyse is met name vereist voor een verwerking waarbij nieuwe technologieën worden gebruikt, die gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt. Denk bijvoorbeeld aan grootschalige verwerking en de verwerking van biometrische gegevens.[34]

Op basis van de PIA moet de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. Denk daarbij aan versleuteling van gegevens, het beschermen van vertrouwelijkheid, het regelmatig testen en evalueren van de beveiliging.[35]

De verwerkingsverantwoordelijke en de verwerker zorgen dat iedere werknemer die toegang heeft tot persoonsgegevens, deze slechts in opdracht van de verwerkingsverantwoordelijke verwerkt.[36] De arbeidsovereenkomstenwet legt aan de werknemers een algemene plicht tot vertrouwelijkheid op.[37] Het opnemen van een meer expliciete vertrouwelijkheidsclausule in de arbeidsovereenkomst en het bieden van een opleiding aan de werknemers zijn zinvolle maatregelen.

## J. MELDINGSPLICHT

Blijkt uit de PIA dat er een groot risico bestaat, dan moeten de verwerkingsverantwoordelijke en de verwerker de GBA raadplegen. De GBA zal een schriftelijk advies geven indien het risico onvoldoende wordt onderkend of beperkt.[38]

## K. SANCTIES

De GDPR versterkt de sancties in vergelijking met de vroegere Belgische privacywet. De vroegere privacycommissie kon niet sanctioneren. Rechtbanken aanvaardden in bepaalde omstandigheden toch onrechtmatig verkregen bewijs, bijvoorbeeld bij een ontslag om dringende reden.[39] Eerder uitzonderlijk kenden rechters een (beperkte) morele schadevergoeding toe aan individuele werknemers omdat hun (vroegere) werkgever de privacywetgeving niet had gerespecteerd.
Vanaf 25 mei 2018 moet de verwerkingsverantwoordelijke kunnen aantonen dat de beginselen inzake de verwerking van persoonsgegevens werden nageleefd.[40] U moet als werkgever-verwerkingsverantwoordelijke

dus het bewijs kunnen leveren dat de verwerking van de persoonsgegevens plaatsvindt conform de GDPR.

Een werknemer kan een klachtenprocedure opstarten bij de GBA. Die kan de werkgever-verwerkingsverantwoordelijke vervolgens een administratieve geldboete opleggen.[41]

**VOORBEELD 1**

Voor het niet correct bijhouden van een register van verwerkingsactiviteiten bedraagt die boete max. € 10.000.000 of (voor een onderneming) tot 2 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar (indien dit cijfer hoger is).

**VOORBEELD 2**

De boete voor het verwerken van gevoelige persoonsgegevens zonder toestemming van de betrokkene (zonder dat een andere uitzondering toepasselijk is) bedraagt max. € 20.000.000 of (voor een onderneming) tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar (indien dit cijfer hoger is).

## L. U KUNT NU AAN DE SLAG

De Belgische regering heeft een wetsontwerp uitgewerkt om de GDPR te concretiseren voor België. Dat betekent niet dat u nog kunt wachten. GDPR trad in werking op 25 mei 2018 en alle verplichtingen gelden nu reeds. Het is trouwens opvallend dat het voorstel weinig aandacht heeft voor de bescherming van persoonsgegevens in het kader van de arbeidsrelatie.

Partena Professional assisteert u graag bij de implementatie van de GDPR in het kader van de arbeidsrelatie binnen uw onderneming. Contacteer ons via legal.partners@partena.be.

**Yves Stox,** Senior Legal Counsel

1 De CBPL stelde een meer uitgebreid stappenplan voor Algemene verordening gegevensbescherming – Bereid je voor in 13 stappen: https://gdpr-eu.be/wp-content/uploads/2016/12/STAPPENPLAN-NL-V2.pdf

2 Art. 6.1.a GDPR.

3 Art. 4.11 GDPR.

4 Art. 7.1 GDPR.

5 Overweging 155 GDPR.

6 Art. 7.3 GDPR.

7 Art. 27 kb van 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

8 Art. 7.2. GDPR.

9 Art. 6.1.b GDPR.

10 Art. 6.1.c GDPR.

11 Art. 6.1.f GDPR.

12 Overweging 47 GDPR.

13 Art. 9.1 GDPR.

14 Overweging 51 GDPR.

15 Dat is ook de positie van de GBA.

16 Art. 9.2 GDPR.

17 Art. 10 GDPR en art. 10 wetsontwerp van 11 juni 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

18 FOD Justitie, Omzendbrief nr. 204 (C – 2013/09204), Uittreksels van het strafregister.

19 Commissie voor Bescherming van de Persoonlijke Levenssfeer Advues 08 / 2002, 11 februari 2002, 3: "Bij gebrek aan een gepaste regelgeving mag de werkgever of het bemiddelingskantoor enkel met de toestemming van de betrokken persoon kennis nemen van de inhoud van het getuigschrift zonder nota ervan te nemen of een vermelding terzake te bewaren, aangezien het tonen en het lezen van een document in beginsel niet onder het toepassingsgebied van de wet vallen."

20 Art. 30.1 GDPR.

21 Ook de verwerker van persoonsgegevens, bijvoorbeeld het sociaal secretariaat, moet een register van de verwerkingsactiviteiten opmaken en bijhouden (art. 30.2 GDPR).

22 Art. 30.5 GDPR.

23 De Commissie voor de bescherming van de persoonlijke levenssfeer, Aanbeveling 06/2017 betreffende het Register van de verwerkingsactiviteiten (CO-AR-2017-011), 6-7.

24 Art. 30.3 GDPR.

25 Art. 30.4 GDPR.

26 Art. 30.1 GDPR.

27 U moet de individuele ontvangers dus niet identificeren.

28 Art. 13-14 GDPR.

29 Art. 11-13 wet op de arbeidsreglementen.

30 Het gewoon personeelsregister moet in de regel niet worden bijgehouden door werkgevers die onder het toepassingsgebied van DIMONA (onmiddellijke aangifte van tewerkstelling in de sociale zekerheid) vallen. Op die manier geven ze al hun gegevens over de in- en uitdiensttreding van personeel elektronisch door.

31 De rechtsvorderingen die uit de arbeidsovereenkomst ontstaan, verjaren 1 jaar na het eindigen van deze overeenkomst of 5 jaar na het feit waaruit de vordering is ontstaan, zonder dat deze termijn 1 jaar na het einde van deze overeenkomst mag overschrijden (art. 15 arbeidsovereenkomstenwet).

32 Art. 44-50 GDPR.

33 Art. 37 GDPR.

34 Art. 35 GDPR; Overweging 91 GDPR.

35 Art. 32.1 GDPR. Zie ook art. 25 GDPR in verband met Gegevensbescherming door ontwerp en door standaardinstellingen (privacy by design en privacy by default).

36 Art. 32.4 GDPR.

37 Art. 17, 3° arbeidsovereenkomstenwet. Zie ook Nationale Arbeidsraad, Advies Nr. 2.087, Voorontwerp van wet betreffende de bescherming van bedrijfsgeheimen.

38 Art. 36 GDPR.

39 Het Hof van Cassatie oordeelde in de Antigoonrechtspraak dat de rechter de toelaatbaarheid van een onrechtmatig verkregen bewijs beoordeelt, rekening houdende met de elementen van de zaak in haar geheel genomen. De rechter moet rekening houden met de wijze waarop het bewijs werd verkregen en de omstandigheden waarin de onrechtmatigheid werd begaan. De rechter mag het bewijsmateriaal niet zomaar negeren. Tenzij wanneer een op straffe van nietigheid voorgeschreven vorm is miskend, mag een dergelijk bewijs alleen worden geweerd wanneer de bewijsverkrijging is aangetast door een gebrek waardoor de betrouwbaarheid ervan wegvalt of waardoor het recht op een eerlijk proces in het gedrang kan worden gebracht (Cass. 10 maart 2008, S.07.0073.N).

40 Art. 5.2 GDPR.

41 Art. 83 GDPR.

ACTUALITEIT

# STARTERSLONEN: UITSTEL

Jongeren aanwerven wordt goedkoper, maar nog niet vanaf 1 juli 2018

In het aprilnummer leest u meer over deze nieuwe maatregel. Nu wordt de implementatie van die maatregel uitgesteld. Het bedrag van de forfaitaire nettovergoeding ligt nog steeds niet vast. Misschien worden een aantal modaliteiten zelfs nog aangepast...

Ook al treedt de maatregel formeel in werking op 1 juli 2018, in de praktijk blijven de starterslonen voorlopig dode letter.

**Yves Stox,** Senior Legal Counsel

ACTUALITEIT

# BEDRIJFSSMARTPHONE EN SPLIT BILL: DE FISCUS VERDUIDELIJKT

Enige tijd geleden stelde de minister van Financiën dat een werknemer geen belastingen op het voordeel van de bedrijfssmartphone betaalt bij een split bill-regeling. In een recente circulaire licht de FOD Financiën dit standpunt toe.[1]

## UITGANGSPUNT

Wanneer een werkgever een split bill-regeling hanteert voor het mobiel telefoon- en internetabonnement, ontstaat er voor het persoonlijk gebruik van de mobiele telefoon (het toestel) geen voordeel van € 36/jaar.

## WAT IS EEN SPLIT BILL-REGELING?

Deze regeling houdt in dat de werknemer rechtstreeks en afzonderlijk van de provider een factuur ontvangt voor het privégebruik van het mobiel telefoon- en internetabonnement.

Een regeling waarbij de werkgever rechtstreeks een factuur ontvangt voor het beroeps- en privégebruik van het telefoon- en internetabonnement en de werknemer de kosten van het privégebruik terugbetaalt (bv. via inhouding op het nettoloon) aan de werkgever maakt geen split bill-regeling uit.

## SPLIT BILL-REGELING VOLGENS ERNSTIGE NORMEN EN CRITERIA

Enkel voor zover de split bill-regeling is vastgesteld overeenkomstig ernstige normen en criteria en dus overeenstemt met de werkelijkheid is er geen voordeel voor de mobiele telefoon.

1 Circulaire 2018/C/63 over de voordelen van alle aard voor het persoonlijk gebruik van een PC, tablet, internetaansluiting, mobiele telefoon of vast of mobiel telefoonabonnement.

Bij een split bill-regeling met een grensbedrag waarboven elke gebruik wordt geacht privégebruik te zijn, moet de werkgever bijgevolg het bewijs leveren dat hij dit grensbedrag vastlegde overeenkomstig ernstige normen en criteria.

**VOORBEELD 1**

Een werkgever stelt een smartphone met een mobiel telefoon- en internetabonnement ter beschikking aan een werknemer. Voor beide abonnementen stelt hij grensbedragen in waarboven elk gebruik geacht wordt privégebruik te zijn. Voor het mobiel telefoonabonnement bedraagt het grensbedrag € 10/maand, voor het mobiel internetabonnement 2 gigabyte/maand. De werkgever stelde deze grensbedragen vast overeenkomstig ernstige normen en criteria. De werknemer ontvangt van de provider rechtstreeks en afzonderlijk een factuur van de provider voor het privégebruik. Dergelijke regeling maakt een split bill-regeling uit.
Er ontstaat bijgevolg geen voordeel van alle aard voor de terbeschikkingstelling van de smartphone en het mobiel telefoon- en internetabonnement.

**VOORBEELD 2**

Een werkgever stelt een smartphone met een mobiel telefoonabonnement ter beschikking aan een werknemer. Wie een privégesprek wil voeren, moet eerst een bepaald cijfer intoetsen vooraleer hij het telefoonnummer intoetst.
Op die manier worden de beroepsmatige gesprekken van de privégesprekken onderscheiden.
De werknemer ontvangt van de provider rechtstreeks en afzonderlijk een factuur voor het privégebruik. Dergelijke regeling is een split bill-regeling.
Er ontstaat bijgevolg geen voordeel van alle aard voor de terbeschikkingstelling van de smartphone en het mobiel telefoon- en internetabonnement.

Kan de werkgever niet het bewijs leveren dat hij het grensbedrag vastlegde overeenkomstig ernstige normen en criteria, dan ontstaat alsnog een belastbaar voordeel van alle aard voor het persoonlijk gebruik van de mobiele telefoon en het mobiel telefoon- en internetabonnement.
De kosten voor het privégebruik die door de provider in het kader van split bill-regeling afzonderlijk en rechtstreeks aan de werknemer werden gefactureerd, mogen dan als een eigen bijdrage in mindering worden gebracht van het voordeel van alle aard.

## SPLIT BILL-REGELING ZOWEL VOOR HET TELEFOONABONNEMENT ALS VOOR HET INTERNETABONNEMENT

Stelt de werkgever zowel een telefoon- als internetabonnement ter beschikking, dan geldt het standpunt op voorwaarde dat de split bill-regeling van toepassing is op beide abonnementen.

Wanneer de split bill-regeling slechts op één van beide ter beschikking gestelde abonnementen van toepassing is, geldt het standpunt niet.

**VOORBEELD**

Een werkgever stelt een smartphone met een mobiel telefoon- en internetabonnement ter beschikking aan een werknemer.
De werknemer mag deze abonnementen voor privédoeleinden gebruiken. Voor het mobiel telefoonabonnement stelt de werkgever een grensbedrag van € 10/maand in waarboven elk gebruik geacht wordt privégebruik te zijn. De werkgever stelde dit grensbedrag vast overeenkomstig ernstige normen en criteria. Voor het mobiel internetabonnement legt hij geen grensbedrag vast (er is m.a.w. geen split bill-regeling voor dit abonnement). De werknemer ontvangt van de provider rechtstreeks en afzonderlijk een factuur van de provider voor het privégebruik van mobiel telefoonabonnement. In dit geval is er wel een terbeschikkingstelling van een mobiel internetabonnement en ontstaat bijgevolg een belastbaar voordeel van € 60/jaar.
Ook voor het persoonlijk gebruik van de smartphone ontstaat een belastbaar voordeel van € 36/jaar. Het standpunt dat geen voordeel voor de smartphone ontstaat geldt immers enkel wanneer er een split bill-regeling is zowel voor het telefoonabonnement als voor het internetabonnement.

## EN OP SOCIAAL VLAK?

Het blijft afwachten of de RSZ eenzelfde standpunt zal innemen op vlak van de bedrijfssmartphone en de split bill-regeling.

**Peggy Criel,** Legal Counsel


PART&NA
PROFESSIONAL