AVG VOOR DE WERKGEVER

In De Belgische Beenhouwerij nr.4 van 8 april 2018 werd een algemeen artikel met betrekking tot de Algemene Verordening Gegevensbescherming (AVG) gepubliceerd.
Hieronder vindt u enige uitleg met betrekking tot uw verplichtingen wanneer u personeel tewerkstelt.

Als werkgever verwerkt u persoonsgegevens van uw personeel *(naam, adres, foto, online profiel, loongegevens, rijksregisternummer, login-gegevens van de computer...enz.).*

Onder '**verwerken**' wordt o.a. verstaan: opslaan, verzamelen, bijwerken, wijzigen, gebruiken, raadplegen, doorzenden, vastleggen, verzamelen, verspreiden, wissen, doorsturen met bedoeling om deze in een bestand op te nemen (digitaal of handmatig (bijvoorbeeld fichebak, een kaft, een kartonnen doos, ...)

Onder persoonsgegevens verstaat met de gegevens op basis waarvan een persoon kan worden geïdentificeerd.

Voorbeelden: *loon- en personeelsadministratie, bewaren van een personeelsdossier, bijhouden van een database van sollicitanten/werknemers/uitzendkrachten, aanwezigheidsregistratiesystemen (badgesystemen, prikklokken), camerabewaking, track&trace systeem in de bedrijfswagen, fotoboek van de werknemers op intranet, gegevens over de familiale situatie van een werknemer, foto's van het personeelsfeest, login gegevens van computersystemen, gegevens van bedrijfsgsm's die de werknemer mag gebruiken voor privégebruik, e-mailpaswoorden, geolokalisatiesystemen ...*

INFORMEER UW WERKNEMERS

Het is verplicht om volgende gegevens mee te delen aan uw werknemers:

- **wie verantwoordelijk is** voor de verwerking van de persoonsgegevens (dit is de werkgever);
- **welke de doeleinden van de verwerking zijn** (waarom de gegevens worden verwerkt);
- **wie de gegevens verwerkt** (d.w.z. wie de gegevens mag verwerken van de werkgever bijv. sociaal secretariaat, arbeidsongevallenverzekeraar, externe dienst voor preventie en bescherming op het werk, controlearts, ..., enz.);
- **welke gegevens** worden verwerkt;
- **waar deze gegevens werden gehaald** (van de werknemer zelf of uit andere bronnen)
- de relevante **rechtsgrond** om de persoonsgegevens te verwerken; (in veel gevallen zal de rechtsgrond terug te vinden zijn in een wettelijke basis)
- het recht om zijn toestemming in te trekken; (enkel indien u geen wettelijke basis heeft)
- de **termijn van opslag** van deze gegevens (hoe lang worden ze bewaard)
- het recht om deze gegevens **over te dragen;**
- **wie de werknemer kan contacteren** over de verwerking van zijn gegevens;
- het **recht op inzage, verbetering, wissen, beperking, bezwaar;**
- het **recht** om **een klacht** in te dienen bij de GBA (Gegevensbeschermingsautoriteit – dit is de opvolger van de Commissie voor Bescherming van Persoonlijke Levenssfeer de zgn. 'Privacycommissie');
- de gegevens van een **privacy officer** (als er één is) (zie verder);
- of de gegevens **buiten de EU** verstuurd zullen worden, en, indien ze buiten de EU verstuurd worden, wat zijn rechten zijn;
- personeelsgegevens centraal wordt opgeslagen op een server van het hoofdkantoor in het buitenland).

U moet de bovenstaande gegeven aan de werknemer **proactief informeren**.

U moet deze info ook schriftelijk en transparant **meedelen** aan de werknemer.

De makkelijkste wijze om de mededelingsplicht te vervullen is om in uw arbeidsreglement een **privacy policy** te laten invoegen (via de procedure tot wijziging van arbeidsreglement).

DOCUMENTEER DE RECHTSGROND VOOR DE VERWERKING

Via de ondertekende privacy policy bekomt u van uw werknemer te toestemming om zijn gegevens te verwerken.

Deze toestemming vormt dan de rechtsgrond op basis waarvan u de gegevens kan en mag verwerken.

Indien de werknemer weigert om zijn toestemming te verlenen, heeft u in bepaalde gevallen toch het recht om de gegevens van de weigerachtige werknemer te verwerken, nl. indien u een gerechtvaardigd belang of wettelijke grond kan aantonen.
Belangrijk is in ieder geval dat u de 'rechtsgrond' documenteert en motiveert waarom u meent een beroep te kunnen doen op een bepaalde rechtsgrond. Deze dient u dan op te nemen in het dataregister (zie hieronder) en dient u mee te delen aan uw werknemers via uw informatieverplichting (zie hierboven).

LEG EEN DATAVERWERKINGSREGISTER AAN

U moet een intern **dataverwerkingsregister** bewaren en actueel bijhouden door periodieke bijwerking.
Dit register kan schriftelijk maar mag ook digitaal worden bijgehouden binnen uw bedrijf.
Het is geen publiek document maar blijft intern.

Hierin moet u **alle processen waarin u persoonsgegevens verwerkt,** beschrijven en per proces de volgende zaken meedelen:

- wie verantwoordelijk is voor de verwerking van de persoonsgegevens;
- welke gegevens worden verwerkt;
- van wie gegevens worden verwerkt;
- de reden van verwerking van de gegevens;
- wie de gegevens ontvangt (bv. het

sociaal secretariaat in het kader van de loonadministratie);
- de bewaartermijn ervan;
- de beveiligingsmaatregelen (bijv. wordt de informatie versleuteld? Zijn databases alleen toegankelijk met een wachtwoord? Welke personen in de organisatie hebben een wachtwoord? Hoe gaat u datalekken opsporen, rapporteren en onderzoeken ? ...enz.)

U moet **alleen regelmatige en frequente** verwerkingen van personeelsgegevens vermelden in het register (uitzondering: indien u meer dan 250 werknemers in dienst heeft). U moet het register van tijd tot tijd actualiseren telkens wanneer er zich wijzigingen voordoen. U vindt een model van dergelijk register terug via de link: https://www.privacycommission.be/nl/model-voor-een-register-van-de-verwerkingsactiviteiten

BESCHERM DE PERSOONSGEGEVENS

U moet de gegevens zo veilig mogelijk verwerken (door ze bv. te anonimiseren, pseudonimiseren of encrypteren).

U moet ook de nodige voorzorgen nemen tegen datalekken (= vermijden dat verkeerde personen de gegevens van uw personeel in handen krijgen).

Het is belangrijk dat u uw **personeel opleidt en sensibiliseert.** Leid hen op zodat iedereen weet hoe om te gaan met persoonsgegevens binnen de organisatie.
Voorbeelden van datalekken: hacking en cybercriminaliteit, maar ook toevallige lekken (een e-mail werd per ongeluk naar een verkeerde ontvanger verzonden, een bedrijfslaptop wordt gestolen, notities worden vergeten op de trein, USB-stick wordt verloren,...enz.).

U moet een intern document, een **register van datalekken**, bijhouden van de datalekken *(omschrijving van het lek, wanneer het plaatsvond, wat gebeurde met de gegevens, van welke (groep) personen werden gegevens gelekt, van hoeveel personen, welke soorten gegevens, gevolgen van de inbreuk, (preventieve)maatregelen die werden genomen, ...enz.)*

Indien er sprake is van een datalek dat waarschijnlijk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moet u melding maken aan de GBA.
Datalekken die een hoog risico vormen voor de betrokkene, moeten gemeld worden aan de betrokkene zelf.

EXTERNE PARTIJEN

Wanneer u een beroep doet op derden om persoonsgegevens van uw personeel te verwerken, dan moet u er zeker van zijn dat deze 'gegevensverwerker' in orde is met de GDPR.
(bijvoorbeeld: sociaal secretariaat, arbeidsongevallenverzekeraar, externe IT-dienstverleners, (arbeidsongevallen)verzekeraar, uitzendbureau, externe dienst voor preventie en bescherming op het werk, pensioenfonds, maaltijdchequebedrijf, een selectie en wervingsbureau, een archiveringsdienst voor e-filing, een cloudservice provider voor de opslag van gegevens, een bewakingsfirma,...)
U moet met deze 'gegevensverwerker' (bijv. uw sociaal secretariaat) **een contract sluiten** waarin u de **nodige garanties** moeten krijgen dat de verwerker de GDPR-wetgeving respecteert.
Breng de diverse leveranciers die persoonsgegevens van uw onderneming verwerken in kaart en sluit met ieder van hen een contract om er zeker van te zijn dat zij de regels rond GDPR naleven zodat de gegevens van uw personeel veilig beschermd zijn bij hen.

TIPS OM CONCREET TE WERK TE GAAN

1. Kijk naar de huidige stand van zaken binnen uw bedrijf: Welke persoonsgegevens verwerkt u op dit ogenblik van het personeel? Waar komen deze gegevens vandaan? Met wie deelt u ze? Wie heeft hiertoe toegang? Lijst deze info op.

2. Op basis van de lijst bekijkt u per gegevenscategorie die u bijhoudt of u een wettelijke grond of de toestemming heeft van de werknemer om de gegevens te verwerken (rechtsgrond).

3. Informeer uw werknemers over de verwerkingsactiviteiten. Geef hen hierover de nodige uitleg en zorg voor schriftelijke informatie via aanpassing van uw arbeidsreglement (en desgevallend andere policies).

4. Breng de risico's op verlies, diefstal of ongeoorloofde toegang en de mogelijke gevolgen d daarvan in kaart. Sensibiliseer uw personeel en leid hen op om op een correcte manier met persoonsgegevens van collega's, klanten, e.d. om te gaan.
Neem desgevallend maatregelen om de gegevens te beveiligen: nieuwe afspraken of technische of organisatorische aanpassingen nodig (toegang tot data beperken, veiligheidsprocedures invoeren, policies voor gebruik van eigen pc of laptop ...).

5. Maak een lijst van organisaties of derden waaraan u persoonsgegevens van uw werknemers overmaakt (bijvoorbeeld sociale secretariaten, verzekeraars, externe diensten voor preventie en bescherming op het werk,...) en zorg ervoor dat u met ieder van hen een contract sluit met daarin een minimum aantal verplichte afspraken en vermeldingen inzake GDPR.

6. Maak het dataregister op en werk dit bij telkens wanneer er zich een wijziging voordoet: het dataregister biedt een overzicht van de verwerking van gegevens, gekoppeld aan doeleinden per verwerkingsprocedure.

7. Maak een register van datalekken, beschrijf daarin welke maatregelen u neemt om deze te voorkomen.

8. Wordt u geconfronteerd met een datalek? maak melding aan de betrokkene en eventueel aan de GBA. Vermeld het datalek in het datalekregister en omschrijf welke acties u ondernam om de schade te beperken/voorkomen.

SANCTIES

Bent u vanaf 25 mei 2018 als werkgever niet in orde met de GDPR, dan riskeert u een boete.

ANDERE BELGISCHE WETGEVING

In België bestaat reeds wetgeving die werknemers beschermen tegen de verwerking van hun persoonsgegevens:
- Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens;
- C.A.O 68 – camerabewaking;
- C.A.O. 81 – controle op de elektronische online communicatiegegevens (gebruik e-mail, internet, enz.);
- C.A.O. 89 – diefstalpreventie en uitgangscontrole.

Opgelet: als u alle maatregelen heeft genomen om GDPR-conform te zijn als werkgever, maar u heeft nog camera's in de onderneming, u wenst controle te doen op het e-mail- en internetgebruik door uw werknemers, ... dan zal u tevens de bijkomende verplichtingen in voornoemde nationale cao's moeten naleven.
Bron : NSZ