GDPR – Privacy Policy

Juli 2019

INHOUDSOPGAVE

PRIVACY BELEID

Dit privacy beleid (het '**privacy beleid**') geeft gegevens over de manier waarop Marlux/STRADUS persoonsgegevens verwerkt van sollicitanten, indien u voor het bedrijf werkt of als u zaken doet met het bedrijf.

Persoonsgegevens worden verwerkt overeenkomstig de Wet bescherming persoonsgegevens (Europese wetgeving 2016/679) en andere toepasselijke nationale en Europese privacywet- en regelgeving (samen de '**wet op gegevensbescherming**').

Vetgedrukte termen in dit privacy beleid zijn opgenomen in de woordenlijst in Bijlage 1.

1. TOEPASSINGSBEREIK

Dit privacy beleid is van toepassing op alle persoonsgegevens die we als gegevensbeheerder verwerken.

Het bedrijf is een gegevensverwerker van dergelijke persoonsgegevens, voor zover het bedrijf besluit waarom en hoe persoonsgegevens verwerkt worden.

Het bedrijf kan persoonsgegevens verwerken van, bijvoorbeeld, werknemers, voormalige werknemers en hun familieleden, tijdelijke werknemers, zelfstandigen, sollicitanten, aannemers, leveranciers, klanten en bezoekers.

2. DOEL

Het doel van dit privacy beleid is uitleggen welke persoonsgegevens we verwerken en hoe en waarom we deze verwerken. Daarnaast geeft dit privacy beleid aan wat onze plichten en verantwoordelijkheden zijn met betrekking tot de bescherming ervan.

Dit privacy beleid is geen uitputtende verklaring van onze acties op het gebied van gegevensbescherming. We geven een aantal praktische varianten aan.

*[voor zover de nationale wet bescherming persoonsgegevens (de '**nationale wet**') relevant is voor dit privacy beleid en/of Marlux/STRADUS (het '**bedrijf**') persoonsgegevens verwerkt op een manier die afwijkt van wat in dit privacy beleid staat (bijv. met betrekking tot de categorieën persoonsgegevens die verwerkt worden, doel van verwerken, etc.,) worden gegevens van dergelijke specifieke verwerkingen aangegeven in Bijlage 2.]*

1. SOORTEN PERSOONSGEGEVENS

1.1 Werknemers, sollicitanten en aannemers

Het bedrijf verzamelt en verwerkt persoonsgegevens met betrekking tot onze (voormalige) werknemers, sollicitanten en (voormalige) aannemers. Deze persoonsgegevens omvatten: persoonsgegevens zoals naam, geboortedatum, rijksregisternummer, bankgegevens, naaste familie, gegevens van sociale media-accounts, visum-/paspoortgegevens; contactgegevens zoals adres en telefoonnummer(s); personeelsdossier met informatie over bijvoorbeeld arbeidsvoorwaarden, training, beoordelingen, promoties, persoonlijke ontwikkelingsplannen, gedrag en disciplinaire gegevens, werklocatie, salarisgegevens, bankrekening, belasting- en sociale zekerheidsinformatie, veiligheidsvrijwaringen; werknemersgeschiedenis/sollicitatiedetails (uit sollicitatiebrieven, curriculum vitae en sollicitatieformulieren) zoals scholing en werkgeschiedenis; redactionele of journalistieke content zoals koppelingen naar werk, bijv. koppelingen naar videobestanden of audiobestanden; medische informatie zoals medische certificaten en absentiebriefjes; familiegegevens zoals namen en geboortedata van kinderen (bijv. relevant als iemand een aanvraag doet voor ouderschapsverlof); details die vereist zijn voor pensioen; details met betrekking tot lidmaatschap van de vakbond; en prestatie gerelateerde gegevens zoals prestatiewaarderingen voor managers en jaarlijkse salarisgesprekken met werknemers, psychometrische tests, etc. De bovenstaande lijst is niet uitputtend, maar bevat de meest gebruikelijke persoonsgegevens die verzameld, gebruikt en verwerkt worden.

1.2 Leveranciers en klanten

Het bedrijf verzamelt en verwerkt persoonsgegevens met betrekking tot onze leveranciers en klanten en/of personen die met hen werken. Deze persoonsgegevens kunnen omvatten: persoonsgegevens zoals naam, titel, functie, werkidentificatienummers, afdeling, business unit (inclusief contactgegevens die verzameld zijn voor training/verificatie); en contactgegevens zoals e-mailadres, telefoonnummer(s) en werklocatie; en belastinginformatie zoals btw-/belastingnummers.

1.3 Speciale categorieën persoonsgegevens

De soorten speciale categorieën van persoonsgegevens die het bedrijf mogelijk verwerkt zijn, zonder beperking, gezondheidsgegevens, gegevens over criminele veroordelingen en biometrische gegevens. Het bedrijf verwerkt alle persoonsgegevens in overeenstemming met de Wet bescherming persoonsgegevens. Dit geldt in het bijzonder voor speciale categorieën persoonsgegevens. [*meer informatie over de soorten persoonsgegevens en **speciale categorieën persoonsgegevens** die door ons verwerkt worden is te vinden in Bijlage 2*.]

2. DOELEN VAN VERWERKING

Het bedrijf verwerkt persoonsgegevens voor het doel/de doelen waarvoor de persoonsgegevens verkregen zijn. Veel voorkomende voordelen van de redenen waarom het bedrijf persoonsgegevens verzamelt zijn: salaris- en uitkeringsadministratie; Personeelszaken, prestatie- en talentbeheer; marketing en PR; verbetering van zakelijke producten en diensten; onderzoek en analyse van statistieken; bedrijfsstrategie; interne audits of onderzoeken; preventie en detectie van illegaal en/of crimineel gedrag richting ons of onze klanten en werknemers; en/of het nakomen van juridische verplichtingen. We kunnen af en toe ook om andere redenen persoonsgegevens verwerken. Het bedrijf probeert ervoor te zorgen dat mensen geïnformeerd worden over het (de) doel(en) waarvoor hun persoonsgegevens verwerkt worden op het moment dat het bedrijf om toestemming vraagt. Als dit niet mogelijk of praktisch is, dan probeert het bedrijf u zo snel mogelijk na de verwerking van de persoonsgegevens te informeren. Personen mogen hun toestemming altijd intrekken.

3. PROFILEREN

Het bedrijf kan persoonsgegevens van verschillende personen (bijvoorbeeld werknemers, aannemers en sollicitanten) verwerken voor talentbeheer en personeelsevaluatie (mogelijk voor het insluiten van aanwezigheids- en prestatieanalyses).

Het bedrijf houdt zich bezig met dergelijke verwerking als: (a) dit uitdrukkelijk toegestaan wordt volgens de nationale wetgeving (inclusief voor het monitoren van fraude of belastingontduiking); (b) het noodzakelijk is voor het aangaan van een of de uitvoering van een contract; of (c) de persoon de nodige toestemming heeft gegeven. [*meer informatie over het type profilering dat we uitvoeren is te vinden in Bijlage 2*.]

4. INDIVIDUELE RECHTEN

Onder de Wet bescherming persoonsgegevens hebben mensen bepaalde rechten.

4.1 **Inspectie en toegang**: u mag ons vragen om een samenvatting en kopie van uw persoonsgegevens die we verwerken of die namens ons verwerkt worden;

4.2 **Correctie/toevoeging/verwijdering**: als u denkt dat uw persoonsgegevens onjuist of onvolledig zijn, dan heeft u het recht ons te vragen om een correctie, wijziging of verwijdering van uw persoonsgegevens;

4.3 **Bezwaar:** u mag bezwaar aantekenen tegen de verwerking van uw persoonsgegevens door ons, op basis van onze legitieme redenen voor de verwerking (zie deel Doelen Van Verwerking hierboven);

4.4 **Beperking:** u kunt van ons vragen dat wij de verwerking van uw persoonsgegevens beperken als de nauwkeurigheid van uw persoonsgegevens in twijfel wordt getrokken, onze verwerking niet rechtmatig is, als u meent dat we de persoonsgegevens niet langer nodig hebben of als u bezwaar hebt aangetekend tegen verwerking; en

4.5 **Geautomatiseerde besluitvorming:** als het bedrijf geautomatiseerde besluitvorming toepast (inclusief profilering) die een aanzienlijke invloed op u heeft, dan mag u bezwaar aantekenen tegen dergelijke besluitvorming.

De Procedure individuele rechten van het bedrijf geeft aan hoe de bovenstaande aanvragen ingediend kunnen worden en hoe het bedrijf deze aanvragen beheert.

5. BEVEILIGING

5.1 Veiligheidsmaatregelen

Het bedrijf heeft technische en organisatorische maatregelen getroffen om persoonsgegevens te beschermen tegen illegale of ongeautoriseerde vernietiging, verlies, wijziging, openbaarmaking, acquisitie of toegang.

Persoonsgegevens worden veilig bewaard via een aantal veiligheidsmaatregelen, waaronder - indien van toepassing - fysieke maatregelen zoals vergrendelde archiefkasten en verschillende IT-maatregelen.

Voor meer informatie over de veiligheidsmaatregelen van het bedrijf leest u het Beleid inzake informatiebeveiliging [*en Bijlage 2*].

5.2 Inbreuk op persoonsgegevens

Het bedrijf zal een inbreuk op persoonsgegevens behandelen overeenkomstig de meldprocedure Inbreuk op persoonsgegevens. Voor informatie over het identificeren en melden van een inbreuk op gegevens leest u onze Procedure inzake inbreuk op persoonsgegevens.

6. BEKENDMAKING PERSOONSGEGEVENS

Af en toe kan het bedrijf persoonsgegevens bekendmaken aan derden of derden toegang geven tot persoonsgegevens die wij verwerken (bijvoorbeeld als een wethandhavingsinstantie of regelgevende instantie een geldig verzoek indient voor toegang tot persoonsgegevens).

Het bedrijf kan ook persoonsgegevens delen: (a) met een ander lid van de CRH Groep (inclusief onze dochterbedrijven, onze uiteindelijke houdstermaatschappij en haar dochterbedrijven); (b) met geselecteerde derde partijen, inclusief zakenpartners, leveranciers en onderaannemers; (c) met derden wanneer we zaken of activa verkopen of kopen; of (d) als het bedrijf een wettelijke verplichting heeft om persoonsgegevens vrij te geven. Dit omvat ook de uitwisseling van gegevens met andere bedrijven en organisaties ten behoeve van fraudepreventie.

Als het bedrijf overeenkomsten aangaat met derden voor het verwerken van persoonsgegevens namens ons, dan zorgt het ervoor dat het contract dusdanig is opgesteld, dat de gegevens voldoende beschermd blijven. Voorbeelden zijn communicatieleveranciers, payroll-dienstverleners, bedrijfsartsen, marketing- of wervingsbureaus, exploitanten van datacentra die door het bedrijf gebruikt worden, etc. [*Meer informatie over de categorieën van derden aan wie het bedrijf persoonsgegevens verstrekt is opgenomen in Bijlage 2.*]

7. GEGEVENSRETENTIE

Het bedrijf bewaart persoonsgegevens zolang dit nodig wordt geacht voor het doel waarvoor de persoonsgegevens verwerkt zijn. Persoonsgegevens worden bewaard in overeenstemming met relevante wetten en bedrijfsrichtlijnen. [*Meer informatie over de retentieperiode voor persoonsgegevens die door het bedrijf aangehouden wordt (of de criteria die worden gebruikt om een dergelijke retentieperiode te bepalen) is opgenomen in Bijlage 2.*]

8. GEGEVENSOVERDRACHT BUITEN DE EER

Af en toe kan het nodig zijn dat het bedrijf persoonsgegevens overdraagt naar een land buiten de EER. Deze overdracht geschiedt in overeenstemming met de toepasselijke wetgeving inzake de bescherming van persoonsgegevens. Het bedrijf neemt alle redelijke stappen om ervoor te zorgen dat persoonsgegevens veilig en - bij overdracht buiten de EER - volgens dit privacy beleid behandeld worden. [*Meer informatie over de aard van gegevensoverdrachten door het bedrijf is opgenomen in Bijlage 2.*]

9. ROLLEN EN VERANTWOORDELIJKHEDEN

Het bedrijf is verantwoordelijk voor het verwerken van persoonsgegevens. De algemeen directeur van het bedrijf heeft een algemene verantwoordelijkheid voor naleving van dit privacy beleid door het bedrijf en zal een primaire contactpersoon aanwijzen voor (i) de verwerking van persoonsgegevens van de huidige en voormalige werknemers en aannemers van het bedrijf; (ii) het verwerken van persoonsgegevens van zakelijke contacten; en (iii) het behoud van de beveiliging en integriteit van de persoonsgegevens die door het bedrijf verwerkt worden.

De afdeling Legal & Compliance zal het bedrijf ondersteunen middels juridisch advies en bijstand in het interpreteren van de wet op bescherming persoonsgegevens en dit privacy beleid op een lokaal niveau.

Alle werknemers van het bedrijf moeten zich houden aan de meest actuele versie van dit privacy beleid, zoals deze af en toe gepubliceerd wordt. Als blijkt dat werknemers bewust dit privacy beleid overtreden hebben, kunnen zij te maken krijgen met disciplinaire maatregelen, tot en met ontslag.

10. KLACHTENPROCEDURE

U kunt een vraag stellen of een klacht indienen over dit privacy beleid en/of de verwerking van uw persoonsgegevens. Neem hiervoor contact op met de GDPR-verantwoordelijke op het nummer +32 13 679 100. Als u bij de relevante toezichthoudende autoriteit [*zoals aangegeven in Bijlage 2*] een klacht indient met betrekking tot onze naleving van de wet op bescherming persoonsgegevens, vragen we u om eerst contact op te nemen met vertrouwenspersoon om ons de kans te geven uw zorgen met u te bespreken.

11. BIJBEHOREND BELEID

Dit beleid dient gelezen te worden in samenhang met het volgende beleid en de volgende procedures:

- Procedure inzake de inbreuk op persoonsgegevens
- Procedure inzake individuele rechten
- Informatiebeveiligingsbeleid
- Privacyverklaring website

Bijlage I

WOORDENLIJST

In dit privacy beleid hebben de onderstaande termen de volgende betekenis:

'**CCM**' verwijst naar de Country Compliance Manager voor het bedrijf;

De '**Europese Economische Ruimte**' of '**EER**' omvat België, Bulgarije, Cyprus, Denemarken, Duitsland, Estland, Finland, Frankrijk, Griekenland, Hongarije, Ierland, IJsland, Italië, Kroatië, Letland, Liechtenstein, Litouwen, Luxemburg, Malta, Nederland, Noorwegen, Oostenrijk, Polen, Portugal, Roemenië, Slovenië, Slowakije, Spanje, Tsjechië, Verenigd Koninkrijk en Zweden.

'**Gegevensverwerker**' verwijst naar de partij die namens de gegevensbeheerder persoonsgegevens verwerkt (bijvoorbeeld een payrollbedrijf).

'**Gegevensbeheerder**' verwijst naar de entiteit die beslist waarom en hoe persoonsgegevens worden verwerkt.

Er is sprake van '**Grensoverschrijdende verwerking**' als: (a) we in meer dan één lidstaat van de EU zijn gevestigd en het verwerken van persoonsgegevens door ons in meer dan één EU-lidstaat plaatsvindt, of (b) als het verwerken van persoonsgegevens in slechts één EU-land plaatsvindt, maar dit (mogelijk) substantiële invloed heeft op personen in meer dan één EU-lidstaat.

'**Inbreuk op persoonsgegevens**' verwijst naar een schending van de beveiliging die leidt tot onbedoeld(e) of onrechtmatig(e) vernietiging, verlies, wijziging, onbevoegde openbaarmaking van of toegang tot verzonden, opgeslagen of anderszins verwerkte persoonsgegevens.

'**Persoonsgegevens**' verwijst naar gegevens betreffende een levend persoon aan de hand waarvan deze persoon kan worden geïdentificeerd. Een persoon is identificeerbaar als zijn/haar identiteit redelijkerwijs kan worden afgeleid aan de hand van de gegevens zonder dat dit een onevenredig grote inspanning kost. Persoonsgegevens kunnen het volgende omvatten:

Werknemers en aannemers

1. Persoonsgegevens zoals naam, geboortedatum, bankrekening, naaste familie, gegevens van sociale media-accounts;

2. Contactgegevens zoals adres en telefoonnummer(s);

3. Personeelsbestandgegevens, waaronder bijv. arbeidsvoorwaarden, training, functioneringsgesprekken, promoties, persoonlijke ontwikkelingsplannen, gedrag en disciplinaire gegevens, werklocatie, salarisgegevens, bankrekening, belasting- en persoonlijk identificeerbare nummers, zoals BSN-nummers;

4. Werkwerknemersgeschiedenis/sollicitatiegegevens zoals scholing en werkgeschiedenis (uit motivatiebrieven, curriculum vitae en sollicitatieformulieren);

5. Redactionele of journalistieke content zoals koppelingen naar werk, bijv. koppelingen naar presentaties of audio-bestanden;

6. Medische informatie zoals medische certificaten en absentiebriefjes;

7. Familiegegevens zoals namen en geboortedata van kinderen, bijv. relevant als iemand een aanvraag doet voor ouderschapsverlof;

8. Gegevens vereist voor pensioen;

9. Gegevens met betrekking tot lidmaatschap van de vakbond; en

10. Prestatie gerelateerde gegevens zoals prestatiebeoordelingen voor managers en jaarlijkse salarisgesprekken van werknemers, psychometrische tests, etc.

Leveranciers en klanten

1. Persoonsgegevens zoals naam, titel, functie, werkidentificatienummers, afdeling, business unit;

2. Contactgegevens zoals e-mailadres, telefoonnummer(s);

3. Werklocatie; en

4. Belastinginformatie zoals btw-/belastingnummers.

'**Profileren**' verwijst naar het geautomatiseerde verwerken van persoonsgegevens met als doel het beoordelen van bepaalde zaken met betrekking tot een persoon om de prestaties, de beslissingen of het gedrag van een persoon te analyseren of voorspellen.

'**Speciale categorieën persoonsgegevens**' verwijst naar soorten persoonsgegevens die de volgende gegevens betreffende een persoon vrijgeven: raciale of etnische oorsprong, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging en lidmaatschap van een vakbond. Speciale categorieën persoonsgegevens omvatten ook het verwerken van genetische gegevens, biometrische gegevens (bijvoorbeeld vingerafdrukken of afbeeldingen van het gezicht), medische gegevens, gegevens betreffende seksleven of seksuele geaardheid en enige persoonsgegevens betreffende strafrechtelijke veroordelingen of feiten.

'**Verwerken**' omvat het op enigerlei wijze verzamelen, gebruiken, vastleggen, organiseren, wijzigen, vrijgeven, vernietigen of bewaren van persoonsgegevens. Verwerken kan handmatig of aan de hand van geautomatiseerde systemen zoals informatietechnologiesystemen gebeuren. De termen '**verwerken**' en '**verwerking**' moeten dienovereenkomstig worden geïnterpreteerd.

Bijlage 2

BEDRIJFSSPECIFIEKE VERWERKING [1]

Deze bijlage bevat aanvullende informatie met betrekking tot de manier waarop het bedrijf persoonsgegevens verwerkt.

1. Relevante lokale wetgevende en toezichthoudende autoriteit

In deze bijlage betekent '**Wet bescherming persoonsgegevens**' de algemene Wet bescherming persoonsgegevens (Verordening (EU) 2016/679). De relevante lokale toezichthoudende autoriteit voor het bedrijf is: **de Belgische Gegevensbeschermingsautoriteit (vroegere Privacy Commissie).**

2. Persoonsgegevens die door het bedrijf verwerkt worden

Naast de categorieën persoonsgegevens die zijn uitgelicht in onderdeel 1 van het privacy beleid, verwerkt het bedrijf ook persoonsgegevens uit de volgende categorieën**:** n.v.t.

3. Doelen van het verwerken van persoonsgegevens

Naast de categorieën persoonsgegevens die zijn uitgelicht in onderdeel 2 van het privacy beleid verwerkt het bedrijf ook persoonsgegevens voor de voldoende doeleinden**:** n.v.t.

4. Profileren

Het bedrijf houdt zich bezig met de volgende soorten profilering: noodzakelijk voor uitbetalen van salarissen, talent management, succession planning, training van medewerkers, toekennen van extralegale voordelen.

5. Veiligheidsmaatregelen

Het bedrijf heeft de volgende technische en organisatorische maatregelen geïmplementeerd om persoonsgegevens te beschermen tegen illegale of ongeautoriseerde vernietiging, verlies, wijziging, openbaarmaking, acquisitie of toegang: automatiseren van dossiers,…

6. Bekendmaking van persoonsgegevens aan derden

Het bedrijf maakt de persoonsgegevens bekend of geeft er toegang toe aan de volgende aanvullende categorieën van derden, voor de hieronder uitgelegde doeleinden: sociaal secretariaat, RSZ, fiscus, arbeidsgeneeskundige dienst, DKV, Vivium, De Federale verzekering, leasemaatschappijen, Total (tankkaarten), arbeidsongevallenverzekering, vakbonden, beroepsfederatie, Edenred, tijdsregistratie, Centhro, Successfactors, Benefits@work. Deze lijst is niet limitatief maar de meest recente is steeds in dataregister te vinden. Deze kan geraadpleegd worden op aanvraag.

7. Gegevensretentieperiodes

Het bedrijf bewaart persoonsgegevens op basis van de volgende criteria: conform wettelijke regels en o.b.v. noodzakelijkheid. Motivatiebrieven, curriculum vitae en gegevens van sollicitatieformulieren worden voor de opbouw van een talentpool voor een periode van 3 jaar bewaard.

8. Gegevensoverdrachten

Het bedrijf draagt persoonsgegevens over aan de volgende locaties buiten de EER, voor de hieronder aangegeven doeleinden. Hierbij worden de aangegeven juridische beschermingsmaatregelen toegepast (een kopie hiervan is beschikbaar via HR): US (SuccessFactors).

PROCEDURE INZAKE DE INBREUK OP PERSOONSGEGEVENS

1. INLEIDING

Deze procedure inzake de inbreuk op persoonsgegevens (de '**procedure**') beschrijft het proces voor het escaleren, rapporteren en opnemen van vermoedelijke of daadwerkelijke inbreuk op persoonsgegevens (zoals hieronder aangegeven). Deze procedure is van toepassing op **Marlux** (het '**bedrijf**'). Het doel van deze procedure is ervoor zorgen dat het bedrijf inbreuk op persoonsgegevens (zoals hieronder aangegeven) snel beheerst, zodat de impact van de inbreuk op persoonsgegevens kan worden geminimaliseerd en er tijdig voldaan kan worden aan de wettelijke verplichting om dergelijk inbreuk te melden bij de wetgever en/of perso(o)n(en) die geraakt is/zijn door de inbreuk (in overeenstemming met de Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679) (de '**AVG**').

2. WAT ZIJN PERSOONSGEGEVENS?

Persoonsgegevens zijn gegevens die betrekking hebben op een levende persoon (woonachtig binnen de Europese Economische Ruimte) en aan de hand waarvan deze persoon kan worden geïdentificeerd ('**persoonsgegevens**'). Een persoon is identificeerbaar als zijn/haar identiteit redelijkerwijs kan worden afgeleid aan de hand van de gegevens, zonder dat dit een onevenredig grote inspanning kost. Voorbeelden van persoonsgegevens zijn: naam, adres, geboortedatum, telefoonnummer, rekeningnummer, functie, foto, IP-adres, etc.

3. WAT IS EEN INBREUK OP PERSOONSGEGEVENS?

De AVG definieert inbreuk op persoonsgegevens' als '*een schending van de beveiliging die leidt tot onbedoeld(e) of onrechtmatig(e) vernietiging, verlies, wijziging, onbevoegde openbaarmaking van of toegang tot verzonden, opgeslagen of anderszins verwerkte persoonsgegevens*' ('**inbreuk persoonsgegevens**'). Inbreuk op persoonsgegevens doet zich voor als er sprake is van onrechtmatig(e) of onbedoeld(e) openbaarmaking, verlies of een andere vorm van onrechtmatig(e), onbedoeld(e) of illega(a)l(e) verzameling, gebruik, registratie, opslag of verspreiding van persoonsgegevens. Voorbeelden van inbreuk op persoonsgegevens zijn: verlies of diefstal van een laptop of mobiele telefoon met persoonsgegevens; versturen van een (onbeschermd) Excel-bestand met persoonsgegevens aan een onrechtmatig persoon; afdrukken van salarisinformatie en deze op de printer laten liggen; hacken van een systeem met persoonsgegevens; en/of verlies of diefstal van bestanden; etc.

Een incident waarbij sprake is van inbreuk op de gegevensbescherming wordt beschreven als een '**gegevensincident**'. Als een gegevensincident geen betrekking heeft op persoonsgegevens, dan is het geen inbreuk op persoonsgegevens. Niet alle gegevensincidenten gerelateerd aan persoonsgegevens zijn bovendien inbreuken op persoonsgegevens. Het verlies of de aantasting van persoonsgegevens wordt bijvoorbeeld niet beschouwd als inbreuk op persoonsgegevens als: (i) de persoonsgegevens zijn versleuteld of geanonimiseerd; (ii) er een volledige, up-to-date back-up van de persoonsgegevens is; en (iii) toegang tot de persoonsgegevens wordt gemonitord. Per situatie moet bekeken worden of een gegevensincident ook een inbreuk op persoonsgegevens vormt.

4. WANNEER IS DEZE PROCEDURE VAN TOEPASSING?

Als bij het gegevensincident *geen* persoonsgegevens betrokken zijn, dan is deze procedure niet van toepassing. Als bij het gegevensincident *wel* persoonsgegevens betrokken zijn, dan kan er sprake zijn van inbreuk op persoonsgegevens en is deze procedure van toepassing. Als er twijfel bestaat over of er sprake is van inbreuk op persoonsgegevens, dan dient het bedrijf direct advies in te winnen bij de afdeling Legal & Compliance om de situatie meteen te beoordelen.

5. HOE MELD IK INTERN EEN INBREUK OP PERSOONSGEGEVENS?

Het is belangrijk dat alle daadwerkelijke of vermoedelijke inbreuken op persoonsgegevens direct intern bij CRH gemeld worden, overeenkomstig de volgende stappen:

5.1 Initiële melding

Zodra u merkt dat er sprake is van een daadwerkelijke of vermoedelijke inbreuk op persoonsgegevens, moet u dit direct melden bij de algemeen directeur van het bedrijf (de '**algemeen directeur van het bedrijf**') of rechtstreeks bij de afdeling Legal & Compliance. De algemeen directeur van het bedrijf zal daadwerkelijke of vermoedelijke inbreuken op persoonsgegevens direct melden bij de afdeling Legal & Compliance.

5.2 Responsplanning

Als er sprake is van inbreuk op persoonsgegevens, dan zal de algemeen directeur of een gemachtigde hiervan samenwerken met de afdeling Legal & Compliance om een plan te ontwikkelen om te reageren op de inbreuk op persoonsgegevens. Bijlage 1 toont een stroomschema voor het beheren van een inbreuk op persoonsgegevens.

Bij het ontwikkelen van het relevante responsplan houdt het responsteam rekening met:

- de informatie die ontvangen is via de melding van inbreuk op persoonsgegevens;
- de vereiste maatregelen die direct genomen moeten worden om de inbreuk op persoonsgegevens te beheersen;
- of er een noodzaak is om de relevante autoriteit voor gegevensbescherming ('**DPA**') op de hoogte te stellen van de inbreuk op persoonsgegevens en zo ja; wat er gemeld moet worden;
- de mogelijke gevolgen voor het bedrijf en de personen waarop de inbreuk op persoonsgegevens invloed heeft;
- de maatregelen die het bedrijf op dat moment neemt en/of kan nemen om de schade voor de personen op wie dit invloed heeft te beperken;
- de wijze waarop de personen waarop het invloed heeft op de hoogte worden gesteld van de inbreuk op persoonsgegevens, indien gepast volgens de omstandigheden, en de maatregelen die personen kunnen nemen om verdere schade te beperken;
- of er sprake kan zijn van persoonlijke aansprakelijkheid of aansprakelijkheid van derden, voortvloeiend uit de inbreuk op persoonsgegevens;
- interne (en indien nodig; externe) communicatie en de timing van dergelijke communicatie;
- of, buiten de DPA, andere aandeelhouders geïnformeerd moeten worden; en
- welke lessen getrokken kunnen worden uit de inbreuk op persoonsgegevens en welke maatregelen geïmplementeerd kunnen worden om te voorkomen dat dit weer gebeurt.

5.3 Melding bij de DPA vereist?

Niet elke inbreuk op persoonsgegevens hoeft gemeld te worden bij de DPA. Het is bijvoorbeeld niet noodzakelijk om de DPA op de hoogte te stellen als de inbreuk op persoonsgegevens waarschijnlijk geen risico vormt voor (een) perso(o)n(en).

Als het noodzakelijk is om de inbreuk op persoonsgegevens te melden bij de relevante DPA, dan zal de afdeling Legal & Compliance de inbreuk op persoonsgegevens eerst bespreken met de algemeen directeur en daarna melden bij de relevante DPA.

De melding bij de relevante DPA dient direct gedaan te worden, waar mogelijk niet later dan 72 uur nadat u gemerkt hebt dat er sprake is van inbreuk op persoonsgegevens. Als er niet binnen 72 uur een melding gedaan wordt, dan moet de DPA hiervoor een onderbouwde reden krijgen.

5.4 Oplossing

Na het doen van de melding bij de relevante DPA en rekening houdend met eventuele opmerkingen van die DPA, zal de afdeling Legal & Compliance de inbreuk op persoonsgegevens en het beheer en de oplossing ervan eerst bespreken met de algemeen directeur, rekening houdend met het relevante responsplan voor inbreuk op persoonsgegevens.

6. WAT MOET BIJ DE DPA GEMELD WORDEN?

Bij het doen van een melding moet de DPA op de hoogte worden gesteld van:

- de aard van de inbreuk op persoonsgegevens, inclusief de categorieën van persoonsgegevens en betrokken personen, het aantal personen dat hierdoor geraakt wordt en het aantal persoonsgegevens dat gecompromitteerd is;
- de waarschijnlijke gevolgen die verwacht kunnen worden als gevolg van de inbreuk op persoonsgegevens;
- de genomen of voorgestelde maatregelen met betrekking tot de inbreuk op persoonsgegevens;
- de maatregelen die genomen kunnen worden door de geraakte personen om schadelijke gevolgen die voortkomen uit de inbreuk op persoonsgegevens te beperken; en
- de naam en contactgegevens van de contactpersoon van CRH, bij wie meer informatie verkregen kan worden met betrekking tot de inbreuk op persoonsgegevens.

7. MELDING INBREUK OP PERSOONSGEGEVENS AAN GETROFFEN PERSONEN

De getroffen persoon hoeft alleen geïnformeerd te worden als een inbreuk op de persoonsgegevens waarschijnlijk kan resulteren in een ‘groot risico’ voor de rechten en vrijheden van het gegevenssubject. Het melden van de inbreuk op persoonsgegevens bij geraakte personen gebeurt volgens het relevante responsplan.

De melding die verstuurd wordt naar geraakte personen omvat, ten minste: (i) de aard en mate van de gegevensinbreuk; (ii) de maatregelen die genomen worden om de negatieve gevolgen van de inbreuk op persoonsgegevens te beperken; (iii) een beschrijving van de vastgestelde en aangenomen gevolgen van de inbreuk op persoonsgegevens; en (iv) de maatregelen die het bedrijf heeft genomen of voorgesteld om de gevolgen van de inbreuk op persoonsgegevens te verminderen.

Meldingen aan personen zijn niet vereist als: (a) het bedrijf passende technische en organisatorische maatregelen heeft geïmplementeerd om ervoor te zorgen dat de persoonsgegevens niet leesbaar zijn voor mensen zonder autorisatie, bijvoorbeeld via versleuteling; of (b) het bedrijf aansluitende maatregelen genomen heeft die ervoor zorgen dat het grote risico voor de personen waarschijnlijk niet materialiseert.

8. GEGEVENSINBREUKREGISTER

Het bedrijf moet een register bijhouden met daarin alle inbreuken op persoonsgegevens. De afdeling Legal & Compliance houdt een register bij met inbreuk op persoonsgegevens waarvan het door het bedrijf op de hoogte wordt gesteld, (elk een ‘**register**’).

Het doel van het register voor inbreuk op persoonsgegevens is: (i) leren van de inbreuk op persoonsgegevens en van de manier hoe ermee omgegaan is; (ii) in staat zijn om juiste antwoorden te geven op vragen van getroffen personen en/of de DPA, waar van toepassing; en (iii) de DPA een samenvatting geven als hierom gevraagd wordt.

Voor elke inbreuk op persoonsgegevens kan het volgende opgenomen worden in het register:

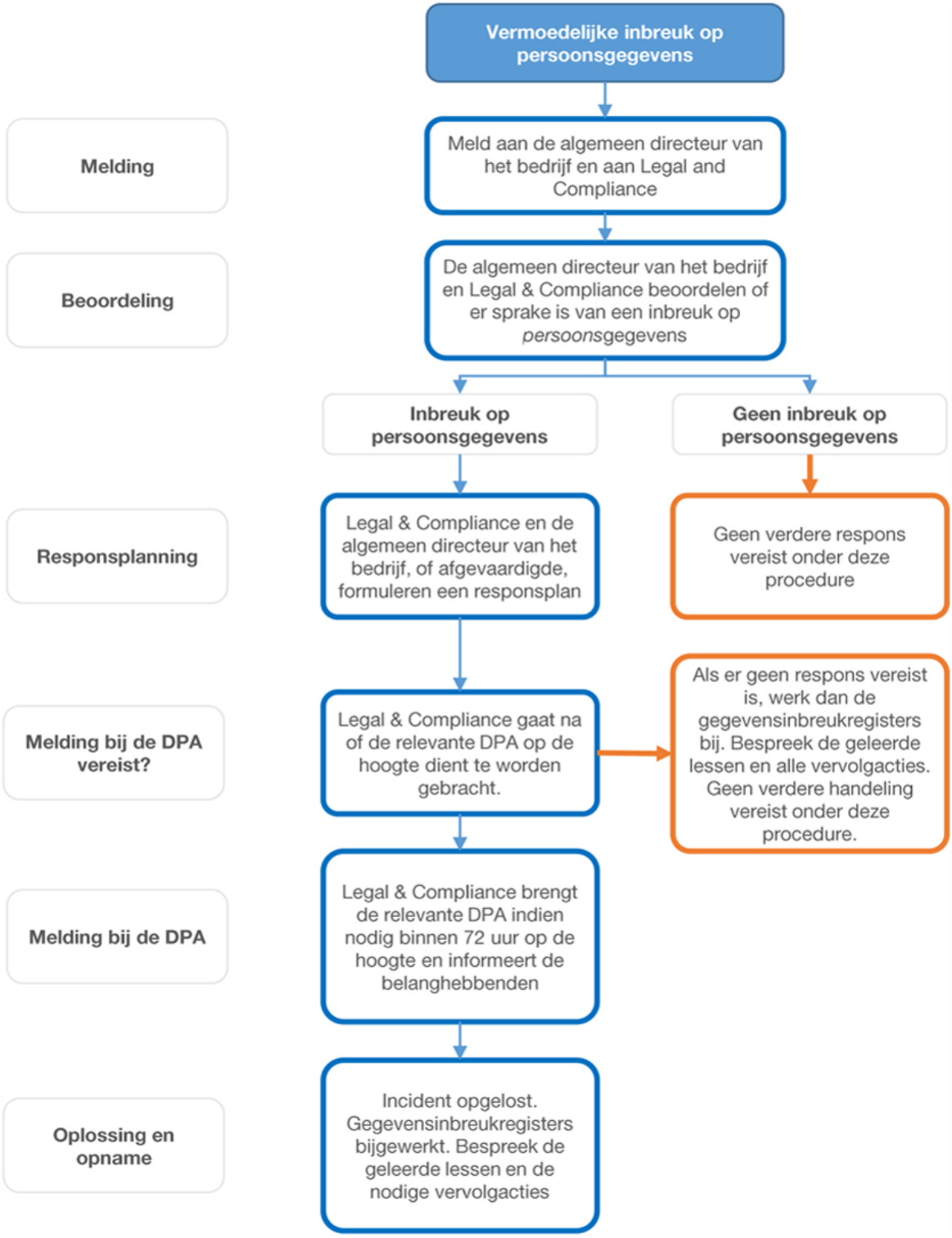
- datum en tijd van de melding van de inbreuk op persoonsgegevens;
- naam en contactgegevens van de getroffen perso(o)n(en);
- de feiten en details van de aard van de inbreuk op persoonsgegevens;
- aan wie de inbreuk op persoonsgegevens gemeld is en waarom; en
- de vervolgacties na ontdekking van de inbreuk op persoonsgegevens (bijvoorbeeld maatregelen om te voorkomen dat een inbreuk op persoonsgegevens opnieuw plaatsvindt, etc.).

Het bedrijfsregister met inbreuken die gemeld zijn bij de DPA moet ten minste vijf jaar bewaard worden.

Bijlage 1

Stroomschema procedure inzake de inbreuk op persoonsgegevens

Mocht u vragen of hulp nodig hebben, neem dan contact op met de afdeling HR of uw (plaatselijke) DPO. U kunt bij de afdeling Legal & Compliance terecht voor advies over de uitwerking van deze procedure.



RECHTEN INZAKE BESCHERMING PERSOONSGEGEVENS EN AANVRAGEN VAN PERSONEN

De Algemene Verordening Gegevensbescherming ('**AVG**') biedt een breed spectrum aan rechten voor personen met betrekking tot hun persoonsgegevens (de '**Individuele Rechten**'). Als gevolg daarvan kunnen personen aanvragen doen voor het evalueren, bewerken, verwijderen, corrigeren van of bezwaar aantekenen tegen het verwerken van hun persoonsgegevens.

Het doel van dit document is: (1) uitleggen wat deze Individuele Rechten zijn; en (2) uitleggen hoe een aanvraag van een persoon om dergelijke Individuele Rechten (een '**aanvraag**') uit te oefenen overeenkomstig de AVG of andere toepasselijke wetgeving, kan worden beheerd. Het stroomschema in de bijlage van dit document helpt bij het illustreren van hoe aanvragen kunnen worden beheerd.

1. INDIVIDUELE RECHTEN

De Individuele Rechten onder de AVG omvatten:

A. Recht op toegang

Elk exploiterend bedrijf (de '**OpCo**'), moet, als Gegevensbeheerder op verzoek van een persoon:

- bevestigen of het de persoonsgegevens van die persoon verwerkt;
- uitleggen waarom en hoe het de persoonsgegevens van die persoon verwerkt en die persoon voorzien van overige gegevens met betrekking tot de persoonsgegevens van die persoon; en
- een kopie van de persoonsgegevens aan die persoon verstrekken.

B. Recht op wissen (ook bekend als het recht op Verwijdering of 'het recht om vergeten te worden') en Rectificatie

Een persoon mag in bepaalde omstandigheden vragen om het 'wissen' of 'verwijderen' van zijn/haar persoonsgegevens, als hij/zij op enig moment zijn/haar toestemming voor de verwerking van zijn/haar persoonsgegevens intrekt (en de verwerking wordt uitgevoerd in navolging van toestemming van het gegevenssubject). De persoon kan ook aan de OpCo vragen om zijn/haar persoonsgegevens te 'rectificeren' of aan te passen als deze onjuist of onvolledig zijn.

Als de OpCo de persoonsgegevens heeft gedeeld met een derde partij (bijvoorbeeld een gegevensverwerker, zoals een payroll-dienstverlener), dan moet de OpCo zo'n derde partij op de hoogte stellen van het wissen of beperken van de relevante persoonsgegevens.

C. Recht op beperking

Een persoon mag de OpCo ook vragen om verwerking van zijn/haar persoonsgegevens te beperken, terwijl klachten (bijvoorbeeld over de juistheid van persoonsgegevens) worden behandeld. Als de verwerking beperkt is, dan mag de OpCo de persoonsgegevens opslaan, maar niet verder verwerken tenzij of tot het probleem is opgelost. Als de OpCo de persoonsgegevens heeft gedeeld met een derde partij (bijvoorbeeld een gegevensverwerker, zoals een payroll-dienstverlener), dan moet de OpCo zo'n derde partij op de hoogte stellen van de beperking op het verwerken van persoonsgegevens van die persoon, tot nader order. De derde partij moet ook op de hoogte worden gesteld als de beperking wordt opgeheven.

D. Recht op bezwaar

Personen kunnen bezwaar indienen tegen de verwerking van hun persoonsgegevens op basis van redenen die samenhangen met zijn of haar specifieke situatie. De OpCo dient verwerking van deze persoonlijke gegevens vervolgens te staken, tenzij deze kan aantonen dat er sprake is van dwingende legitieme gronden voor het verwerken van deze gegevens (dit moet per geval worden bepaald).

Personen kunnen echter bezwaar maken zonder hiervoor een rechtvaardiging te geven als een OpCo de gegevens verwerkt voor directe marketingdoeleinden.

Als er een beslissing wordt gemaakt betreffende geautomatiseerde verwerking van persoonlijke gegevens, inclusief profielbepaling, en als die beslissing mogelijk juridische gevolgen heeft voor de persoon of als deze aanzienlijke gevolgen heeft voor hem/haar, dan heeft de persoon het recht om niet onderhevig te zijn (behoudens enkele specifieke uitzonderingen) aan een beslissing die *alleen* op die basis wordt gemaakt. Voorbeelden van dergelijke automatische verwerking zijn online kredietbesluiten.

E. Gegevensportabiliteit

Als een persoon de OpCo zijn/haar persoonlijke gegevens verstrekt, heeft de persoon op verzoek het recht om:

- een kopie van de persoonlijke gegevens te ontvangen; en/of
- indien technisch mogelijk, de persoonlijke gegevens in een gestructureerde en vaak gebruikte geautomatiseerde indeling naar een externe partij te laten verzenden.

2. BEHEER VAN VERZOEKEN

A. Reageren op een verzoek

De OpCo moet de persoon die het verzoek heeft ingediend en met een externe partij waarmee de persoonlijke gegevens zijn gedeeld, op de hoogte brengen zodra de wijziging, verwijdering of beperking is uitgevoerd.

Informatie of communicatie die voortvloeiend uit een verzoek aan personen wordt verstrekt:

- moet bondig, duidelijk en eenvoudig te begrijpen zijn, in gemakkelijk toegankelijke vorm zijn en in gewone taal zijn opgesteld;
- moet schriftelijk zijn (bv. een brief of e-mail); en
- mag indien mogelijk, als een persoon op digitale wijze een verzoek indient (bv. via e-mail), ook in elektronische vorm worden verstrekt (bv. via e-mail), tenzij de persoon anders verzoekt.

B. Deadline voor reageren op een verzoek

Na ontvangst van een geldig verzoek dient de reactie ‘zonder onnodig uitstel’ te worden verstrekt, maar in ieder geval niet later dan een maand na ontvangst van het verzoek. Die periode van een maand kan indien nodig met nog eens twee maanden worden verlengd, waarbij rekening dient te worden gehouden met de complexiteit en het aantal verzoeken. De OpCo dient de persoon binnen een maand na ontvangst van het verzoek op de hoogte te brengen van een dergelijke verlenging, waarbij ook de redenen voor de vertraging/verlenging dienen te worden vermeld. Als de OpCo een geldige en legitieme reden heeft om binnen het uiteengezette tijdsbestek of überhaupt niet op een verzoek te reageren, dient deze: (a) de persoon ‘onverwijld’ op de hoogte te brengen van de redenen waarom geen actie wordt ondernomen; dit in ieder geval niet later dan een maand na ontvangst van het verzoek; en (b) de persoon op de hoogte te brengen van zijn/haar recht om een klacht in te dienen bij de relevante gegevensbeschermingsautoriteit.

C. Kosten voor reageren op een verzoek

Alle informatie/communicatie van de OpCo betreffende een verzoek dient kosteloos te verlopen, tenzij het verzoek van de persoon als ‘*kennelijk ongegrond of buitensporig*’ (bv. herhaaldelijke verzoeken) kan worden aangemerkt. In een dergelijk geval kan de OpCo: (a) de persoon redelijke kosten in rekening brengen; of (b) het verzoek weigeren.

D. Nog vragen?

Als u nog vragen of meer hulp nodig hebt, kan de OpCo om hulp vragen bij de afdeling HR of de (plaatselijke) functionaris voor gegevensbescherming (Data Protection Officer, DPO). U kunt bij de afdeling Legal en Compliance terecht voor advies over de uitwerking van deze procedure.

U kan steeds uw rechten uitoefenen door contact op te nemen met de verantwoordelijke GDPR van Marlux/STRADUS op het nummer : +32 13 679 100.

Bijlage 1

Beheer van verzoeken m.b.t. persoonlijke gegevens - stroomdiagram

Mocht u vragen hebben of hulp nodig hebben, neem dan contact op met de afdeling HR of uw (plaatselijke) DPO. U kunt bij de afdeling Legal en Compliance terecht voor advies over de uitwerking van deze procedure.