Gegevensbeveiligingsbeleid

Experts in perimeter protection

Privacybeleid

Dit privacybeleid (het 'privacybeleid') bevat details over de manier waarop Heras B.V. ('het bedrijf',) persoonsgegevens verwerkt wanneer je voor het bedrijf werkt of wanneer je zaken doet met het bedrijf.

Persoonsgegevens worden verwerkt in overeenstemming met de Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679) en andere toepasselijke nationale en Europese privacywet- en regelgeving (samen de 'wetgeving inzake gegevensbescherming'). De vetgedrukte termen die in dit privacybeleid worden gebruikt, zijn opgenomen in de verklarende woordenlijst in bijlage I.

1. Toepassingsgebied

Dit privacybeleid is van toepassing op alle persoonsgegevens die wij als verwerkingsverantwoordelijke verwerken.

Voor zover het bedrijf beslist waarom en hoe persoonsgegevens worden verwerkt, is het bedrijf een verwerkingsverantwoordelijke van die persoonsgegevens.

Het bedrijf kan persoonsgegevens verwerken van bijvoorbeeld werknemers, voormalige werknemers en hun gezinsleden, uitzendkrachten, zelfstandigen, sollicitanten, contractanten, contactpersonen bij leveranciers, klanten en bezoekers.

2. Doel

In dit privacybeleid leggen wij uit welke persoonsgegevens wij verwerken en hoe en waarom wij deze verwerken. Daarnaast schetsen wij in dit privacybeleid onze plichten en verantwoordelijkheden met betrekking tot de bescherming hiervan.
Dit privacybeleid is geen alomvattende verklaring van onze praktijken inzake gegevensbescherming. Voor zover mogelijk brengen wij je op de hoogte van afwijkingen. [voor zover de nationale wetgeving inzake gegevensbescherming (de 'nationale wetgeving') relevant is voor dit privacybeleid, en/of Heras (het 'bedrijf') persoonsgegevens verwerkt op een manier die afwijkt van wat in dit privacybeleid is uiteengezet (bijvoorbeeld met betrekking tot de categorieën verwerkte persoonsgegevens, de doeleinden van de verwerking, enz.), zijn details van dergelijke verwerking opgenomen in bijlage II.]

1. Type persoonsgegevens

1.1 Werknemers en contractanten

Het bedrijf verzamelt en verwerkt persoonsgegevens met betrekking tot onze werknemers, sollicitanten en contractanten, evenals voormalige werknemers en voormalige contractanten. Deze persoonsgegevens omvatten: persoonlijke gegevens zoals naam, geboortedatum, bsn, bankrekeninggegevens, naaste familie, details van socialemedia-accounts, visum-/paspoortgegevens; contactgegevens zoals adres en telefoonnummer(s); gegevens uit het personeelsdossier, zoals arbeidsvoorwaarden, opleiding, prestatiebeoordelingen, promoties, persoonlijke ontwikkelingsplannen, gedragsgegevens en disciplinaire maatregelen, werklocatie, salarisinformatie, bankrekeninggegevens, belastingnummer en bsn, veiligheidsmachtigingen; arbeidsverleden/sollicitatiegegevens zoals opleidingsgeschiedenis en arbeidsverleden; redactionele of journalistieke inhoud, bijv. links naar werken, zoals links naar video- of audiobestanden; medische informatie zoals medische attesten en ziekmeldingen; familiegegevens zoals namen en geboortedata van kinderen (bijvoorbeeld relevant als iemand ouderschapsverlof aanvraagt); gegevens die vereist zijn voor pensioen; gegevens over vakbondslidmaatschap; en prestatiegerelateerde gegevens zoals prestatiebeoordelingen voor managers en jaarlijkse salarisverhoging van werknemers, psychometrische tests, enz. De bovenstaande lijst is niet volledig, maar omvat de persoonsgegevens die het meeste worden verzameld, gebruikt en anderszins verwerkt.

1.2 Leveranciers en klanten

Het bedrijf verzamelt en verwerkt persoonsgegevens van onze leveranciers en klanten en/of personen die samenwerken met onze leveranciers en klanten. Deze persoonsgegevens kunnen bestaan uit: persoonlijke gegevens zoals naam, titel, functie, werkidentificatienummers, afdeling, bedrijfseenheid (inclusief voor training/verificatie verzamelde contactgegevens); en contactgegevens zoals e-mailadres, telefoonnummer(s) en werklocatie; en fiscale informatie zoals btw-/belastingnummers.

1.3 Bijzondere persoonsgegevenscategorieën

De typen bijzondere persoonsgegevenscategorieën die het bedrijf mogelijk verwerkt, omvatten, zonder beperking, gezondheidsgegevens, informatie over strafrechtelijke veroordelingen en biometrische gegevens. Het bedrijf verwerkt alle persoonsgegevens, en met name bijzondere persoonsgegevenscategorieën, in overeenstemming met de wetgeving inzake gegevensbescherming.

[nadere bijzonderheden over de typen persoonsgegevens en bijzondere persoonsgegevenscategorieën die wij verwerken zijn opgenomen in bijlage II.]

2. Doeleinden van de verwerking

Het bedrijf verwerkt persoonsgegevens voor het doel of de doelen waarvoor de persoonsgegevens zijn verkregen.

Bekende voorbeelden van redenen waarom het bedrijf persoonsgegevens verwerkt zijn: salarisadministratie en administratie van uitkeringen; HR, prestatie- en talentmanagement; marketing en PR; verbetering van zakelijke producten en diensten; onderzoek en statistische analyse; bedrijfsstrategie; interne audits of onderzoeken; preventie en detectie van onwettig en/of crimineel gedrag naar ons of onze klanten en werknemers; en/of het voldoen aan wettelijke verplichtingen. Van tijd tot tijd verwerken wij persoonsgegevens mogelijk om andere redenen. Het bedrijf probeert ervoor te zorgen dat personen worden geïnformeerd over het doel of de doelen waarvoor hun persoonsgegevens worden verwerkt op het moment dat het bedrijf toestemming verkrijgt. Wanneer dit niet mogelijk of praktisch is, probeert het bedrijf je zo snel mogelijk na de verwerking van persoonsgegevens te informeren. Personen hebben te allen tijde het recht hun toestemming in te trekken.

3. Profilering

Het bedrijf kan de persoonsgegevens van verschillende personen (bijvoorbeeld werknemers, contractanten en sollicitanten) verwerken voor talentmanagement en personeelsevaluatie (waaronder eventueel aanwezigheids- en prestatieanalyses).
Het bedrijf voert deze verwerkingen uit wanneer: (a) dit uitdrukkelijk wordt toegestaan door de nationale wetgeving (inclusief voor controle op fraude en belastingontduiking); (b) dit noodzakelijk is voor het aangaan of uitvoeren van een overeenkomst; of (c) de betrokkene toestemming heeft gegeven. [Nadere bijzonderheden over het type profilering dat wij uitvoeren, zijn opgenomen in bijlage II.]

4. Individuele rechten

Personen hebben bepaalde rechten op grond van wetgeving inzake gegevensbescherming.

4.1 Inzage en toegang: je hebt het recht van ons een overzicht en een kopie te verzoeken van de persoonsgegevens die wij van jou verwerken of namens ons worden verwerkt;
4.2 Correctie/aanvulling/verwijdering: wanneer je van mening bent dat jouw persoonsgegevens onjuist of onvolledig zijn, heb je het recht ons te verzoeken jouw persoonsgegevens te corrigeren, te wijzigen of te verwijderen;
4.3 Bezwaar: je kunt bezwaar maken tegen de verwerking van jouw persoonsgegevens op basis van onze gerechtvaardigde redenen voor verwerking (zie artikel 2 'doeleinden van de verwerking' hierboven);
4.4 Beperking: je kunt ons verzoeken de verwerking van jouw persoonsgegevens te beperken wanneer de juistheid van je persoonsgegevens wordt betwist, onze verwerking onwettig is, je van mening bent dat wij de persoonsgegevens niet meer nodig hebben of je bezwaar hebt gemaakt tegen verwerking; en
4.5 Geautomatiseerde besluitvorming: wanneer het bedrijf geautomatiseerde besluitvorming (met inbegrip van profilering) uitvoert die aanzienlijke gevolgen voor jou heeft, heb je het recht bezwaar te maken tegen dergelijke besluitvorming.

In het artikel 'rechten en verzoeken van individuen inzake gegevensbescherming' leggen we uit hoe bovengenoemde verzoeken kunnen worden ingediend en hoe het bedrijf deze verzoeken afhandelt.

5. Beveiliging

5.1 Beveiligingsmaatregelen

Het bedrijf heeft technische en organisatorische maatregelen ingesteld om persoonsgegevens te beschermen tegen onwettig(e) of onbevoegd(e) vernietiging, verlies, wijziging, openbaarmaking, verwerving of toegang. Persoonsgegevens worden veilig bewaard met behulp van een reeks beveiligingsmaatregelen, waaronder, waar van toepassing, fysieke maatregelen zoals afgesloten archiefkasten.

Zie de jaarlijkse updates [en bijlage II] voor meer informatie over de beveiligingsmaatregelen van het bedrijf.

5.2 Inbreuk in verband met persoonsgegevens

Een gegevenslek zal door het bedrijf worden beheerd in overeenstemming met de procedure voor het rapporteren van inbreuk in verband met persoonsgegevens. Raadpleeg onze procedure voor inbreuk in verband met persoonsgegevens voor advies over hoe je een gegevenslek vaststelt en rapporteert.

6. Openbaarmaking van persoonsgegevens

Het bedrijf kan van tijd tot tijd persoonsgegevens bekendmaken aan derde partijen, of derden toegang geven tot persoonsgegevens die wij verwerken (bijvoorbeeld wanneer een wetshandhavingsautoriteit of regelgevende autoriteit een geldig verzoek indient om toegang tot persoonsgegevens te verkrijgen).

Het bedrijf kan daarnaast persoonsgegevens delen: (a) met een ander lid van de Heras Groep (inclusief onze dochterondernemingen, onze overkoepelende holding en haar dochterondernemingen); (b) met geselecteerde derde partijen, waaronder zakenpartners, leveranciers en onderaannemers; (c) met derde partijen wanneer wij een bedrijf of activa verkopen of kopen; of (d) als het bedrijf wettelijk verplicht is persoonsgegevens bekend te maken. Dit omvat tevens het uitwisselen van informatie met andere bedrijven en organisaties in het kader van fraudepreventie.

Wanneer het bedrijf overeenkomsten aangaat met derde partijen om namens ons persoonsgegevens te verwerken, zal het ervoor zorgen dat er passende contractuele bescherming wordt geboden om deze gegevens te beschermen. Voorbeelden hiervan zijn communicatieproviders, aanbieders van salarisadministratiediensten, aanbieders van bedrijfsgezondheidsdiensten, marketing- of wervingsbureaus, exploitanten van door het bedrijf gebruikte datacenters, enz. [Aanvullende gegevens over de categorieën derde partijen waaraan het bedrijf persoonsgegevens van individuen bekendmaakt, zijn opgenomen in bijlage II.]

7. Gegevensbewaring

Het bedrijf bewaart persoonsgegevens slechts zolang het bewaren van deze persoonsgegevens noodzakelijk wordt geacht in het kader van de doeleinden waarvoor deze persoonsgegevens worden verwerkt. Persoonsgegevens worden bewaard in overeenstemming met de relevante wetgeving en bedrijfsrichtlijnen. [Aanvullende gegevens over de door het bedrijf gevolgde bewaartermijn voor persoonsgegevens (of de criteria die worden gebruikt voor het bepalen van een dergelijke bewaartermijn) zijn opgenomen in bijlage II.]

8. Gegevensdoorgifte buiten de EER

Van tijd tot tijd kan het nodig zijn dat het bedrijf de persoonsgegevens doorgeeft buiten de Europese Economische Ruimte (EER). Deze doorgifte vindt plaats in overeenstemming met de toepasselijke wetgeving inzake gegevensbescherming. Het bedrijf neemt redelijke maatregelen om ervoor te zorgen dat de persoonsgegevens veilig en in overeenstemming met dit privacybeleid worden behandeld wanneer ze buiten de EER worden doorgegeven. [Aanvullende gegevens over de aard van de door het bedrijf uitgevoerde gegevensdoorgifte zijn opgenomen in bijlage II].

9. Rollen en verantwoordelijkheden

Het bedrijf is verantwoordelijk voor de verwerking van persoonsgegevens. De algemeen directeur van het bedrijf is eindverantwoordelijke voor de naleving van dit privacybeleid door het bedrijf en wijst een primair contactpunt aan met betrekking tot (i) de verwerking van persoonsgegevens van huidige en voormalige werknemers en contractanten van het bedrijf; (ii) de verwerking van persoonsgegevens van zakelijke contacten; en (iii) het behoud van de veiligheid en integriteit van de door het bedrijf verwerkte persoonsgegevens.
Alle werknemers van het bedrijf moeten de recentste versie van dit privacybeleid, zoals die van tijd tot tijd wordt gepubliceerd, naleven. Als blijkt dat een werknemer dit privacybeleid opzettelijk heeft geschonden, kan deze worden onderworpen aan disciplinaire maatregelen, tot en met ontslag.

10. Klachtenprocedure

Je kunt een vraag stellen of een klacht indienen over dit privacybeleid en/of de verwerking van jouw persoonsgegevens door contact op te nemen met de HR-manager van Heras.

Bijlage I

Verklarende woordenlijst

In dit privacybeleid hebben de onderstaande termen de volgende betekenis:

‘Grensoverschrijdende verwerking’ ontstaat wanneer: (a) wij in meer dan één EU-lidstaat zijn gevestigd en in meer dan één EU-lidstaat persoonsgegevens verwerken; of b) wij persoonsgegevens weliswaar in slechts één EU-lidstaat verwerken, maar deze verwerking aanzienlijke gevolgen heeft (of waarschijnlijk aanzienlijke gevolgen zal hebben) voor personen in meer dan één EU-lidstaat.

‘Inbreuk in verband met persoonsgegevens’: een inbreuk op de beveiliging die resulteert in onopzettelijk(e) of onwettig(e) vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking van of toegang tot doorgegeven, opgeslagen of anderszins verwerkte persoonsgegevens.

‘Verwerkingsverantwoordelijke’: de entiteit die beslist waarom en hoe persoonsgegevens worden verwerkt.

‘Gegevensverwerker’: de partij die namens de verwerkingsverantwoordelijke persoonsgegevens verwerkt (bijvoorbeeld een aanbieder van salarisadministratiediensten).
‘Europese Economische Ruimte’ of ‘EER’: 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.
‘Persoonsgegevens’: alle gegevens van een levende persoon die het mogelijk maken die persoon te identificeren. Een persoon is identificeerbaar als diens identiteit redelijkerwijs zonder onevenredige inspanning uit de gegevens kan worden afgeleid. Persoonsgegevens kunnen afkomstig zijn van:

Werknemers en contractanten

1. Persoonlijke gegevens zoals naam, geboortedatum, bankrekeninggegevens, naaste familie, gegevens van socialemedia-accounts;
2. Contactgegevens zoals adres en telefoonnummer(s);
3. Gegevens uit het personeelsdossier, zoals arbeidsvoorwaarden, opleiding, prestatiebeoordelingen, promoties, persoonlijke ontwikkelingsplannen, gedragsgegevens en disciplinaire maatregelen, werklocatie, salarisinformatie, bankrekeninggegevens en fiscale en persoonlijk identificeerbare nummers zoals bsn;
4. Arbeidsverleden/sollicitatiegegevens zoals opleidingsgeschiedenis en arbeidsverleden;
5. Redactionele of journalistieke inhoud, bijv. links naar werken, zoals links naar video- of audiobestanden
6. Medische informatie zoals medische attesten en ziekmeldingen;
7. Familiegegevens zoals namen en geboortedata van kinderen, bijvoorbeeld relevant als iemand ouderschapsverlof aanvraagt;
8. Gegevens die vereist zijn voor pensioen;
9. Gegevens over vakbondslidmaatschap; en
10. Prestatiegerelateerde gegevens zoals prestatiebeoordelingen voor managers en jaarlijkse salarisverhoging van werknemers, psychometrische tests, enz.

Leveranciers en klanten

1. Persoonlijke gegevens zoals naam, titel, functie, werkidentificatienummers, afdeling, bedrijfseenheid;
2. Contactgegevens zoals e-mailadres, telefoonnummer(s),
3. Werklocatie; en
4. Fiscale informatie zoals btw-/belastingnummers.

‘Verwerking’: dit omvat het verzamelen, gebruiken, vastleggen, organiseren, wijzigen, bekendmaken, vernietigen of bewaren van persoonsgegevens op welke wijze dan ook. Verwerking kan zowel handmatig plaatsvinden als met behulp van geautomatiseerde systemen, zoals informatietechnologiesystemen en ‘verwerken’ en ‘verwerking’ moeten dienovereenkomstig worden geïnterpreteerd.

‘Profilering’: de geautomatiseerde verwerking van persoonsgegevens met als doel het beoordelen van bepaalde aspecten in verband met een persoon om diens prestaties, beslissingen of gedrag te analyseren of te voorspellen.

‘Bijzondere persoonsgegevenscategorieën’ zijn typen persoonsgegevens die een van de volgende typen informatie over een persoon onthullen: ras of etnische afkomst, politieke overtuiging, godsdienst of levensbeschouwelijke overtuiging, of lidmaatschap van een vakbond. Bijzondere persoonsgegevenscategorieën omvatten ook de verwerking van genetische gegevens, biometrische gegevens (bijvoorbeeld vingerafdrukken of gezichtsopnamen), gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, en persoonsgegevens in verband met strafrechtelijke veroordelingen of strafbare feiten.

Bijlage II

Bedrijfsspecifieke verwerking

Deze bijlage bevat aanvullende informatie over de wijze waarop het bedrijf persoonsgegevens verwerkt.

1. Relevante lokale wetgeving en toezichthouder voor gegevensbescherming

In deze bijlage wordt onder ‘wetgeving inzake gegevensbescherming’ verstaan de Algemene verordening gegevensbescherming (Verordening (EU) 2016/679) en de Nederlandse Wet Bescherming Persoonsgegevens. De relevante lokale toezichthouder voor gegevensbescherming voor het bedrijf is: De Nederlandse Autoriteit Persoonsgegevens

2. Door het bedrijf verwerkte persoonsgegevens

Naast de in artikel 1 van het privacybeleid genoemde categorieën persoonsgegevens verwerkt het bedrijf bovendien de volgende categorieën persoonsgegevens: gegevens met betrekking tot het kenteken van een leaseauto

3. Doeleinden van de verwerking van persoonsgegevens

Naast de in artikel 2 van het privacybeleid beschreven doeleinden verwerkt het bedrijf bovendien persoonsgegevens voor de volgende aanvullende doeleinden: geen aanvullende doeleinden

4. Beveiligingsmaatregelen

Het bedrijf stelt de volgende technische en organisatorische beveiligingsmaatregelen in om persoonsgegevens te beschermen tegen onbevoegd(e) vernietiging, verlies, wijziging, openbaarmaking, verwerving of toegang: geen aanvullende beveiligingsmaatregelen

5. Openbaarmaking van persoonsgegevens aan derde partijen

Het bedrijf maakt de persoonsgegevens openbaar aan of verleent toegang tot de volgende aanvullende categorieën derde partijen voor de hieronder uiteengezette doeleinden: geen aanvullende categorieën

6. Gegevensoverdracht

Het bedrijf geeft persoonsgegevens door aan de locaties buiten de EER, voor de doeleinden die zijn vastgelegd in het Register persoonsgegevens van het bedrijf, met gebruikmaking van de aangegeven wettelijke waarborgen (een exemplaar hiervan is verkrijgbaar bij de HR-directeur van de Groep).

Rechten en verzoeken van personen inzake gegevensbescherming

De Algemene verordening gegevensbescherming ('AVG') voorziet in een groot aantal rechten voor personen inzake hun persoonsgegevens (de 'Individuele Rechten'). Hieruit vloeit voort dat personen verzoeken kunnen indienen om hun persoonsgegevens in te zien, te wijzigen, te wissen, te corrigeren of bezwaar te maken tegen de verwerking ervan.

Het doel van dit document is: (1) uitleggen wat deze individuele rechten zijn; en (2) uitleggen hoe een verzoek van een individu om deze individuele rechten uit te oefenen (een 'verzoek') moet worden afgehandeld in overeenstemming met de AVG of andere toepasselijke wetgeving. Het stroomschema in de bijlage bij dit document illustreert hoe verzoeken kunnen worden beheerd.

1. Individuele rechten

De individuele rechten onder de AVG omvatten:

A. Recht van inzage

Heras-vestigingen in elk land en elke Heras-afdeling is als verwerkingsverantwoordelijke, op specifiek verzoek van een persoon, verplicht tot het volgende:

- bevestigen of de persoonsgegevens van de betrokkene worden verwerkt;
- uitleggen waarom en hoe de persoonsgegevens van die betrokkene worden verwerkt en andere details verstrekken aan die betrokkene met betrekking tot de verwerking van diens persoonsgegevens; en
- een kopie te verstrekken van de persoonsgegevens aan die betrokkene.

B. Recht op gegevenswissing (ook bekend als het Recht op wissing of het Recht op vergetelheid) en rectificatie

In bepaalde omstandigheden kan een betrokkene verzoeken dat diens persoonsgegevens worden 'gewist' of verwijderd, onder meer indien de betrokkene de toestemming voor de verwerking van diens persoonsgegevens intrekt (wanneer de verwerking plaatsvindt met toestemming van de betrokkene). De betrokkene kan de Heras-afdeling ook verzoeken diens persoonsgegevens te 'rectificeren' of te wijzigen indien deze gegevens onjuist of onvolledig zijn.

Indien de Heras-afdeling de persoonsgegevens heeft gedeeld met een derde partij (bijvoorbeeld een gegevensverwerker zoals een aanbieder van salarisadministratiediensten), moet de Heras-afdeling deze derde partij in kennis stellen van het wissen of de beperking ten aanzien van het verwerken van de desbetreffende persoonsgegevens.

C. Recht op beperking

Een betrokkene kan de Heras-afdeling ook verzoeken de verwerking van diens persoonsgegevens te beperken terwijl klachten (bijvoorbeeld over de juistheid van de persoonsgegevens) worden behandeld. Wanneer de verwerking is beperkt, mag de Heras-afdeling de persoonsgegevens opslaan, maar niet verder verwerken, tenzij of totdat de kwestie is afgehandeld. Ook indien de Heras-afdeling de persoonsgegevens heeft gedeeld met een derde partij (bijvoorbeeld een gegevensverwerker zoals een aanbieder van salarisadministratiediensten), moet de Heras-afdeling deze derde partij in kennis stellen van de opgelegde beperking met betrekking tot de verwerking van de desbetreffende persoonsgegevens en deze verwerking tot nader order laten opschorten. Na opheffing van de beperking moet ook de derde partij in kennis worden gesteld.

D. Recht van bezwaar

Betrokkenen kunnen bezwaar maken tegen de verwerking van hun persoonsgegevens om redenen die verband houden met hun bijzondere situatie. De Heras-afdeling dient de verwerking van deze persoonsgegevens in dit geval op te schorten, tenzij kan worden aangetoond dat voor de verwerking dwingende gerechtvaardigde redenen bestaan (per geval te bepalen).

Betrokkenen kunnen echter zonder opgave van redenen bezwaar maken indien een Heras-afdeling de persoonsgegevens verwerkt voor direct marketing.

Indien een besluit wordt genomen op basis van geautomatiseerde verwerking van persoonsgegevens, waaronder profilering, en indien dat besluit voor de betrokkene rechtsgevolgen kan hebben of anderszins aanzienlijke gevolgen kan hebben voor de betrokkene, heeft deze (behoudens enkele specifieke uitzonderingen) het recht niet te worden onderworpen aan een besluit dat uitsluitend is genomen op basis van deze automatische verwerking. Voorbeelden van dergelijke geautomatiseerde verwerking zijn online kredietbeslissingen.

E. Gegevensoverdraagbaarheid

Indien een betrokkene diens persoonsgegevens verstrekt aan een andere Heras vestiging of afdeling, heeft die persoon het recht om, op verzoek:

- een kopie van de persoonsgegevens te ontvangen; en/of
- indien technisch haalbaar, de persoonsgegevens in een gestructureerd en algemeen gebruikte geautomatiseerde vorm naar een derde organisatie te laten doorzenden.

2. Verzoeken beheren

A. Reageren op een verzoek

Zodra de wijziging, verwijdering of beperking is uitgevoerd, moet de Heras-afdeling contact opnemen met de betrokkene die het verzoek heeft ingediend en met elke derde partij aan wie de persoonsgegevens zijn verstrekt.

Gegevens of mededelingen die in reactie op een verzoek aan betrokkenen worden verstrekt:

- moeten zijn opgesteld in een beknopte, duidelijke, eenvoudig te begrijpen en gemakkelijk toegankelijke vorm, in gewone taal;
- moeten schriftelijk worden verstrekt (bijvoorbeeld per brief of e-mail); en
- mogen, wanneer de betrokkene het verzoek in elektronische vorm indient (bijv. per e-mail), tevens in elektronische vorm (d.w.z. per e-mail) worden verstrekt, tenzij de betrokkene anders verzoekt.

B. Termijn voor het beantwoorden van een verzoek

Na ontvangst van een geldig verzoek moet het antwoord worden verstrekt ‘zonder onnodige vertraging’, maar in ieder geval niet later dan een maand na ontvangst van het verzoek. Deze termijn van een maand kan, indien nodig, met twee maanden worden verlengd, rekening houdend met de complexiteit en het aantal verzoeken. De Heras-afdeling moet de betrokkene binnen de eerste maand na ontvangst van het verzoek in kennis stellen van een dergelijke verlenging, samen met de redenen voor deze vertraging/verlenging.

Indien de Heras-afdeling een geldige en gerechtvaardigde reden heeft om niet binnen de voorgeschreven termijn te antwoorden, of om hierop helemaal niet te antwoorden, moet deze (a) de betrokkene ‘onverwijld’ in kennis stellen van de redenen waarom geen er actie wordt ondernomen, maar in ieder geval niet later dan een maand na ontvangst van het verzoek; en b) de betrokkene wijzen op diens recht om een klacht in te dienen bij de bevoegde gegevensbeschermingsautoriteit.

C. Kosten voor het beantwoorden van een verzoek

Alle informatie/communicatie door de Heras-afdeling in verband met een verzoek moet gratis zijn, tenzij het verzoek van de betrokkene 'kennelijk ongegrond of buitensporig' is (bijvoorbeeld herhaalde verzoeken), in welk geval de Heras-afdeling: (a) een redelijke vergoeding in rekening mag brengen bij de betrokkene; of b) het verzoek mag weigeren.

D. Vragen?

Heb je vragen of wens je extra ondersteuning? De HR-afdeling van Heras van het betreffende land kan vragen stellen aan Group HR of Group IT over de interpretatie van deze procedure.

Procedure voor inbreuk in verband met persoonsgegevens

1. Inleiding

Deze procedure voor inbreuk in verband met persoonsgegevens (de 'procedure') omvat de procedure voor het escaleren, rapporteren en registreren van vermoedelijke of daadwerkelijke inbreuken in verband met persoonsgegevens (zoals hieronder gedefinieerd). Deze procedure is van toepassing op Heras (het 'bedrijf'). Het doel van deze procedure is ervoor te zorgen dat het bedrijf een inbreuk in verband met persoonsgegevens (zoals hieronder gedefinieerd) snel beheert en inperkt, zodat de impact van de inbreuk op de gegevens tot een minimum kan worden beperkt en een eventuele wettelijke verplichting om de inbreuk op de gegevens te rapporteren aan een toezichthouder en/of een of meer personen die door de inbreuk in verband met de gegevens zijn getroffen (overeenkomstig de Algemene verordening gegevensbescherming (Verordening (EU) 2016/679) (de 'AVG')) tijdig kan worden nageleefd.

2. Wat zijn persoonsgegevens?

'Persoonsgegevens': alle gegevens van een levende persoon (binnen de Europese Economische Ruimte) die het mogelijk maken die persoon te identificeren ('persoonsgegevens'). Een persoon is identificeerbaar als diens identiteit redelijkerwijs zonder onevenredige inspanning uit de gegevens kan worden afgeleid. Voorbeelden van persoonsgegevens zijn: naam, adres, geboortedatum, telefoonnummer, rekeningnummer, functie, foto, IP-adres, enz.

3. Wat is een inbreuk in verband met persoonsgegevens?

De AVG definieert een inbreuk in verband met persoonsgegevens als een inbreuk op de beveiliging die resulteert in onopzettelijk(e) of onwettig(e) vernietiging, verlies, wijziging, ongeoorloofde openbaarmaking van of toegang tot doorgegeven, opgeslagen of anderszins verwerkte persoonsgegevens ('inbreuk in verband met persoonsgegevens'). Een inbreuk in verband met persoonsgegevens doet zich voor wanneer er sprake is van een ongeoorloofde(e) of onopzettelijk(e) bekendmaking, verlies of enige andere vorm van ongeoorloofde, toevallige of onwettige verzameling, gebruik, registratie, opslag of verspreiding van persoonsgegevens. Voorbeelden van inbreuken in verband met persoonsgegevens zijn: verlies of diefstal van een laptop of mobiele telefoon met persoonsgegevens; het verzenden van een (onbeveiligd) Excel-bestand met persoonsgegevens naar een onbevoegd persoon; het afdrukken van loongegevens en deze vervolgens achterlaten op een printer; het hacken van een systeem met persoonsgegevens; en/of verlies of diefstal van bestanden; enz.

Een incident waarbij sprake is van een inbreuk op de gegevensbeveiliging wordt een 'gegevensincident' genoemd. Als een gegevensincident geen betrekking heeft op persoonsgegevens, is het geen inbreuk in verband met persoonsgegevens. Daarnaast zijn niet alle incidenten waarbij persoonsgegevens betrokken zijn, inbreuken in verband met persoonsgegevens. Zo kan het verlies of de compromittering van persoonsgegevens niet worden aangemerkt als een inbreuk in verband met persoonsgegevens als: (i) de persoonsgegevens versleuteld of geanonimiseerd zijn; ii) er een volledige, actuele back-up van de persoonsgegevens is; en iii) de toegang tot de persoonsgegevens wordt bewaakt. Daarom moet per geval worden bepaald of een gegevensincident een inbreuk in verband met persoonsgegevens vormt.

4. Wanneer is deze procedure van toepassing?

Als bij een gegevensincident geen persoonsgegevens betrokken zijn, is deze procedure niet van toepassing. Als bij een gegevensincident persoonsgegevens betrokken zijn, is mogelijk sprake van een inbreuk in verband met persoonsgegevens en is deze procedure van toepassing. Als er enige twijfel bestaat of er sprake is van een inbreuk in verband met persoonsgegevens, moet het bedrijf onmiddellijk advies inwinnen bij de HR-manager van het land en deze verzoeken de situatie onmiddellijk te beoordelen.

5. Hoe rapporteer ik intern een inbreuk in verband met persoonsgegevens?

Het is belangrijk dat alle werkelijke of vermoedelijke inbreuken in verband met persoonsgegevens onmiddellijk intern bij je hoger leidinggevende of aan HR worden gerapporteerd overeenkomstig de volgende stappen:

5.1 Eerste rapportage

Wanneer je bewust wordt van een werkelijke of vermoedelijke inbreuk in verband met persoonsgegevens, moet je dit onmiddellijk rapporteren aan je hoger leidinggevende of aan HR. Deze melden elke werkelijke of vermoedelijke inbreuk in verband met persoonsgegevens onmiddellijk met relevante personen die hierbij betrokken dienen te worden.

5.2 Plannen van de reactie

Als zich een inbreuk in verband met persoonsgegevens heeft voorgedaan, werkt de hoger leidinggevende en/of HR samen om een plan op te stellen in reactie op de inbreuk in verband met persoonsgegevens. Bijlage A bevat een stroomschema voor het beheer van een inbreuk in verband met persoonsgegevens.

Bij de ontwikkeling van het betreffende plan van aanpak houdt het responsteam rekening met:

- de informatie in de kennisgeving betreffende de inbreuk in verband met persoonsgegevens;
- de vereiste maatregelen die onmiddellijk moeten worden getroffen om de inbreuk in verband met persoonsgegevens te beperken;
- of er een verplichting is de relevante gegevensbeschermingsautoriteit ((+31)
- (0)70 - 888 85 00) op de hoogte te stellen van de inbreuk in verband met persoonsgegevens en zo ja, wat er moet worden gerapporteerd;
- de mogelijke gevolgen van de inbreuk in verband met persoonsgegevens voor het bedrijf en de getroffen personen;
- de maatregelen die het bedrijf op dat moment neemt en/of kan nemen om de schade voor de getroffen personen te beperken;
- de wijze waarop de getroffen personen zullen worden geïnformeerd over de inbreuk in verband met persoonsgegevens, indien passend in de omstandigheden, en de maatregelen die de personen kunnen nemen om verdere schade te beperken;
- of er persoonlijke aansprakelijkheid of aansprakelijkheid van derden kan voortvloeien uit de inbreuk in verband met persoonsgegevens;
- interne (en indien nodig externe) communicatie en het moment waarop deze communicatie plaatsvindt;
- of behalve de gegevensbeschermingsautoriteit ook andere stakeholders moeten worden geïnformeerd; en
- welke lessen kunnen worden geleerd uit de inbreuk in verband met persoonsgegevens en welke maatregelen kunnen worden genomen om herhaling te voorkomen.

5.3 Kennisgeving aan de Autoriteit Persoonsgegevens vereist?

Niet elke inbreuk in verband met persoonsgegevens hoeft te worden gemeld aan de Autoriteit Persoonsgegevens (AP). Zo is het niet nodig om de AP in kennis te stellen wanneer het onwaarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor een of meer personen.
Indien de inbreuk in verband met persoonsgegevens moet worden gemeld bij de relevante gegevensbeschermingsautoriteit, zal je hoger leidinggevende en/of HR de inbreuk in verband met persoonsgegevens melden aan de relevante gegevensbeschermingsautoriteit na dit te hebben besproken met de directeur van het bedrijf.

De inbreuk moet zonder onnodige vertraging worden gemeld aan de relevante gegevensbeschermingsautoriteit, en indien mogelijk niet later dan 72 uur nadat het bedrijf zich bewust is geworden van de inbreuk in verband met persoonsgegevens. Als de kennisgeving niet binnen 72 uur wordt gedaan, moet een gemotiveerde rechtvaardiging voor de vertraging aan de AP worden verstrekt.

5.4 Besluit

Na kennisgeving aan de relevante gegevensbeschermingsautoriteit en overwegen van eventuele opmerkingen van die gegevensbeschermingsautoriteit, zal de hoger leidinggevende en/of HR met de directeur van het bedrijf overleggen over het beheer en de oplossing van de inbreuk in verband met persoonsgegevens conform het plan voor de aanpak voor inbreuken in verband met persoonsgegevens.

6. Wat moet aan de gegevensbeschermingsautoriteit worden gerapporteerd?

Wanneer melding wordt gedaan moet de gegevensbeschermingsautoriteit worden geïnformeerd over:

- de aard van de inbreuk in verband met persoonsgegevens, met inbegrip van de betrokken categorieën persoonsgegevens en personen, het aantal getroffen personen en de hoeveelheid gecompromitteerde persoonsgegevens;
- de te verwachten gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die zijn genomen of voorgesteld om de inbreuk in verband met persoonsgegevens aan te pakken;
- de maatregelen die de getroffen personen kunnen nemen om de schadelijke gevolgen van de inbreuk in verband met persoonsgegevens te beperken; en
- de naam en contactgegevens van het contactpunt van Heras B.V. bij wie meer informatie over de inbreuk op de persoonsgegevens kan worden opgevraagd.

7. Kennisgeving van inbreuk in verband met persoonsgegevens aan getroffen personen

Getroffen personen hoeven alleen te worden geïnformeerd als een inbreuk in verband met persoonsgegevens waarschijnlijk een 'hoog risico' inhoudt voor de rechten en vrijheden van de betrokkene. De melding van de inbreuk in verband met persoonsgegevens aan de getroffen personen vindt plaats conform het plan van aanpak.

De kennisgeving aan de getroffen personen moet ten minste het volgende omvatten: i) de aard en de omvang van de inbreuk in verband met persoonsgegevens; ii) de maatregelen die zijn genomen om de negatieve gevolgen van de inbreuk in verband met persoonsgegevens te beperken; iii) een omschrijving van de vastgestelde en veronderstelde gevolgen van de inbreuk in verband met persoonsgegevens; en iv) de maatregelen die het bedrijf heeft genomen of van plan is te nemen om de gevolgen van de inbreuk in verband met persoonsgegevens te beperken.

Kennisgeving aan personen is niet vereist indien: (a) het bedrijf passende technische en organisatorische maatregelen heeft genomen die de persoonsgegevens onbegrijpelijk maken voor personen die niet gemachtigd zijn de gegevens in te zien, bijvoorbeeld door versleuteling; of b) het bedrijf vervolgens maatregelen heeft genomen die ervoor zorgen dat het zeer onwaarschijnlijk is dat het hoge risico voor personen zich zal voordoen.

8. Register van inbreuken in verband met gegevens

Het bedrijf moet een register bijhouden waarin alle inbreuken in verband met persoonsgegevens worden geregistreerd. HR en IT houden een register bij van inbreuken in verband met persoonsgegevens die door het bedrijf aan hen worden gemeld.

Het doel van het register van inbreuken in verband met persoonsgegevens is: (i) leren van de inbreuk in verband met persoonsgegevens en van de manier waarop deze inbreuk is afgehandeld; (ii) nauwkeurige antwoorden kunnen geven op vragen van getroffen personen en/of de gegevensbeschermingsautoriteit, indien van toepassing; en (iii) op verzoek een samenvatting verstrekken aan de gegevensbeschermingsautoriteit.

Voor elke inbreuk in verband met persoonsgegevens worden de volgende gegevens in het register opgenomen:

- datum en tijdstip waarop de inbreuk in verband met persoonsgegevens is gerapporteerd;
- naam en contactgegevens van de getroffen persoon of personen;
- de feiten en bijzonderheden over de aard van de inbreuk in verband met persoonsgegevens;
- aan wie de inbreuk in verband met persoonsgegevens is gemeld en waarom; en
- de vervolgacties na de ontdekking van de inbreuk in verband met persoonsgegevens (zoals maatregelen om te voorkomen dat de inbreuk in verband met persoonsgegevens zich opnieuw voordoet, enz.)

Het register van het bedrijf met alle aan de gegevensbeschermingsautoriteit gemelde inbreuken met betrekking tot persoonsgegevens moet ten minste vijf jaar worden bewaard.

Gepubliceerd door	Heras
Contactpersoon	HR-manager voor het land
Doel	Transparant en conform zakelijk gedrag waarborgen
Toepassing/gedistribueerd naar	Alle werknemers
Classificatie	Openbaar
Toezicht	Uitvoerend comité
Versie	V_1.1
Ondertekend door/op	Het bestuur van Heras