Verwerkersovereenkomst Terborgse HandelsOnderneming B.V.

Inhoud

1.0 Contractpartijen verwerkersovereenkomst Terborgse HandelsOnderneming B.V.

Datum:

Contractspartijen:

1. Naam verantwoordelijke: Terborgse HandelsOnderneming B.V.
   Statutair gevestigd te : Terborg
   Vertegenwoordigd door:

   Hierna te noemen: **"THO"**

Én:

2. Naam verwerker: _____ _____

   Statutair gevestigd te: _____

   Vertegenwoordigd door: _____

   hierna te noemen: **"Partij 2"**

   gezamenlijk aan te duiden als: **"Wij"**

Overwegende dat:

Wij hebben op _____ een overeenkomst met betrekking

tot _____ gesloten.

Ter uitvoering van deze gezamenlijke overeenkomst worden persoonsgegevens verwerkt.

De THO hecht grote waarde aan het beschermen van deze persoonsgegevens, daarom is de THO verantwoordelijk voor de gegevens die partij 2 gaat verwerken en leggen wij in deze verwerkersovereenkomst en de daarbij behorende bijlagen:

1. overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen
2. overzicht met beveiligingsmaatregelen
3. proces rondom het melden van datalekken en de te verstrekken informatie

vast wat partij 2 wel en niet mag doen met de persoonsgegevens.

2.0 Definities

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

2.1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificatie zoals een naam, een identificatienummer, locatiegegevens, een online identificatie of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

2.2 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

2.3 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen ("Verantwoordelijke");

2.4 Verwerker: een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de 2.3 verwerkingsverantwoordelijke persoonsgegevens verwerkt ("Verwerker");

2.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegevens betrekking hebben;

2.6 Verwerkersovereenkomst: deze overeenkomst inclusief de bijlagen ("Verwerkersovereenkomst");

2.7 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit;

2.8 Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens ("Data-lek");

2.9 Gegevensbescherming-effectbeoordeling: het uitvoeren van een beoordeling, voorafgaand aan het uitvoeren van de verwerking, van het effect van de beoogde verwerkingsactiviteiten op de bescherming van de persoonsgegevens.

2.10 Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens;

3.0 Totstandkoming, duur en beëindiging van deze verwerkersovereenkomst

3.1 Deze verwerkersovereenkomst treedt in werking op de datum waarop wij deze ondertekenen.

3.2 Deze verwerkersovereenkomst is onderdeel van de overeenkomst en zal gelden voor zolang de overeenkomst duurt.

3.3 Indien de overeenkomst eindigt, eindigt deze verwerkersovereenkomst automatisch; de verwerkersovereenkomst kan niet apart worden opgezegd.

3.4 Na beëindiging van deze verwerkersovereenkomst zullen de lopende verplichtingen voor partij 2, zoals het melden van Datalekken, waarbij de persoonsgegevens van de THO betrokken zijn, en de plicht tot geheimhouding blijven voortduren.

4.0 Verwerken Persoonsgegevens

4.1 Partij 2 zal alleen persoonsgegevens verwerken in opdracht van de THO en heeft geen zeggenschap over de persoonsgegevens. Partij 2 volgt de instructies van de THO hierover op en partij 2 mag de persoonsgegevens niet op een andere manier verwerken, tenzij de THO partij 2 daar van te voren toestemming of opdracht voor geeft.

4.2 In Bijlage 1 wordt opgenomen welke persoonsgegevens partij 2 precies zal verwerken en voor welke verwerkingsdoeleinden.

4.3 Partij 2 houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.

4.4 Partij 2 mag zonder voorafgaande schriftelijke toestemming van de THO geen andere personen of organisaties inschakelen bij het verwerken van de persoonsgegevens. Een inkooporder met deze (persoons)gegevens mag als toestemming beschouwd worden.

4.5 Wanneer partij 2 met toestemming van de THO andere organisaties inschakelt, moeten deze andere organisaties minimaal voldoen aan de eisen die zijn opgenomen in deze verwerkersovereenkomst.

4.6 Wanneer de THO een verzoek krijgt van een betrokkene die zijn of haar privacy rechten wil uitoefenen, werkt partij 2 daar binnen een termijn van 14 dagen aan mee. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen persoonsgegevens.

4.7 Wanneer de THO partij 2 verzoekt om de THO informatie te verschaffen, dan zal partij 2 de informatie verstrekken die de THO nodig heeft voor het uitvoeren van een gegevensbescherming- effectbeoordeling. De THO heeft dit nodig om in te kunnen schatten wat het risico van de verwerking is die partij 2 namens de THO uitvoert.

5.0 Beveiligen van Persoonsgegevens

5.1 Partij 2 zorgt ervoor dat de persoonsgegevens voldoende beveiligd zijn. Om verlies en onrechtmatige verwerkingen te voorkomen neemt partij 2 passende technische en organisatorische maatregelen.

5.2 Deze maatregelen zijn afgestemd op het risico van de verwerking. Een overzicht van deze maatregelen en het beleid daarover neemt partij 2 op in Bijlage 2.

5.3 Ter controle kan de THO ieder jaar een rapportage opvragen waarin de genomen beveiligingsmaatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor zal partij 2 aan de THO geen kosten in rekening brengen.

5.4 De THO mag op moment er een gegrond vermoeden is dat partij 2 niet conform de AVG handelt, een inspectie of audit in partij 2 haar organisatie laten uitvoeren om te bepalen of het verwerken van de persoonsgegevens aan de wet en de afspraken uit deze verwerkersovereenkomst voldoet. Hierbij zal partij 2 haar medewerking verlenen, waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.

5.5 De kosten voor de uitvoering van deze audit zullen voor rekening van partij 2 komen wanneer blijkt dat partij 2 zich niet aan de verplichtingen in deze verwerkersovereenkomst houdt.

5.6 De controle op de algehele verwerking van persoonsgegevens door partij 2 kan, naast de audit mogelijkheid, ook gebeuren via zelfevaluatie. Partij 2 zal hierbij aan de THO een rapport verstrekken waarin partij 2 aantoont dat partij 2 voldoet aan de wet en de afspraken uit deze verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid uit partij 2 haar organisatie.

5.7 Wanneer de THO of partij 2 vindt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden partijen in overleg over de wijziging daarvan. De kosten voor het wijzigen van de beveiligingsmaatregelen komen voor de rekening van de partij die de kosten maakt.

6.0 Exporteren Persoonsgegevens

6.1 Partij 2 mag geen persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van de THO.

7.0 Geheimhouding

7.1 Partij 2 zal de aan haar verstrekte persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.

7.2 Partij 2 zal ervoor zorgen dat ook haar personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-) contracten op te nemen.

8.0 Data-lekken

8.1 In geval van een ontdekking van een mogelijk data-lek zal partij 2 de THO hierover informeren binnen 24 uur via **privacy@terborgse.nl** en de THO de informatie verstrekken die is aangegeven in Bijlage 3, zodat de THO indien nodig een melding bij de toezichthouder kan doen.

8.2 Na de melding van een data-lek aan de THO, zal partij 2 de THO op de hoogte houden van nieuwe ontwikkelingen rondom het data-lek en de maatregelen die partij 2 heeft getroffen om de omvang van het data-lek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen.

8.3 Eventuele kosten die gemaakt worden om het data-lek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van de partij die de kosten maakt.

9.0 Aansprakelijkheid

9.1 Als partij 2 verplichtingen uit deze verwerkersovereenkomst niet nakomt, stelt de THO partij 2 daarvoor aansprakelijk.

9.2 Partij 2 is aansprakelijk voor alle schade geleden door het niet nakomen van de wet en de bepalingen uit deze verwerkersovereenkomst, voor zover dit is ontstaan door werkzaamheden van partij 2.

9.3 Indien partij 2 de verplichtingen in deze verwerkersovereenkomst overtreedt, is partij 2 aan de THO een direct opeisbare boete verschuldigd van € 1,- voor iedere overtreding en € 0,01 voor iedere dag dat partij 2 de overtreding begaat. Daarnaast behoudt de THO het recht om schadevergoeding te vorderen.

9.4 Partij 2 is aansprakelijk voor de aan de THO opgelegde bestuurlijke boete door de toezichthouder als de geleden schade het gevolg is van onrechtmatig of nalatig handelen door partij 2.

9.5 De THO is niet aansprakelijk voor aanspraken van betrokkenen of andere personen en organisaties waar partij 2 de samenwerking mee is aangegaan of waarvan partij 2 persoonsgegevens verwerkt, als dit het gevolg is van onrechtmatig of nalatig handelen van partij 2.

10.0 Teruggave persoonsgegevens en bewaartermijn

10.1 Na het beëindigen van deze verwerkersovereenkomst geeft partij 2 de persoonsgegevens terug. Eventuele achtergebleven persoonsgegevens zal partij 2 op een zorgvuldige en veilige manier vernietigen.

10.2 De persoonsgegevens die partij 2 verwerkt volgens deze verwerkersovereenkomst zal partij 2 vernietigen na verstrijken van de wettelijke bewaartermijn en/of op verzoek van de THO. Een wettelijke bewaartermijn is er bijvoorbeeld wanneer partij 2 de persoonsgegevens moet bewaren om belastingtechnische redenen.

10.3 De THO kan aan partij 2 om een rapportage vragen na teruggave en/of vernietiging van de persoonsgegevens, waarin partij 2 verklaart dat de persoonsgegevens niet langer in haar bezit zijn.

11.0 Slotbepalingen

11.1 Deze verwerkersovereenkomst is onderdeel van de overeenkomst. Alle rechten en verplichtingen uit de overeenkomst zijn daarom ook van toepassing op de verwerkersovereenkomst.

11.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de verwerkersovereenkomst en de overeenkomst, gelden de bepalingen uit deze verwerkersovereenkomst.

11.3 Afwijkingen van deze verwerkersovereenkomst zijn slechts geldig wanneer de THO en partij 2 dit samen schriftelijk afspreken.

11.4 Op deze verwerkersovereenkomst en de werkzaamheden van partij 2 is het Nederlandse recht van toepassing.

11.5 Over eventuele geschillen tussen de THO en partij 2 bepaalt de rechter in de rechtbank binnen het gebied waar de THO gevestigd is.

Aldus door ons overeengekomen en ondertekend:

Verantwoordelijke:

Ondertekend voor en namens: Terborgse HandelsOnderneming B.V.

Naam: _____

Functie: _____

Datum en plaats: _____

Handtekening: _____

Verwerker:

Ondertekend voor en namens: _____

Naam: _____

Functie: _____

Datum en plaats: _____

Handtekening: _____

Bijlage 1: Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen

Het onderstaande schema zal ingevuld moeten worden elke keer dat een verwerkersovereenkomst wordt gesloten. Het geeft een volledig overzicht van de persoonsgegevens die verwerkt zullen worden. Dit maakt het makkelijker om aan te kunnen tonen waar, door wie en voor welk doel de persoonsgegevens worden verwerkt.

Beschrijving verwerkingsactiviteiten door verwerker:

_____

_____

Verwerkingsdoelen: _____

Verwerkingsverantwoordelijke: _____

Verwerker: _____

Sub verwerkers: _____

Verwerkte Persoonsgegevens: _____

_____

Locatie verwerkingen: _____

Bewaartermijn: _____

Bijlage 2: Overzicht met beveiligingsmaatregelen

Hier moet een overzicht van de beveiligingsnormen opgenomen worden die de verwerkingsverantwoordelijke aan de verwerker opgelegd. Om vast te stellen wat passende beveiligingsmaatregelen zijn moet een afweging worden gemaakt op basis van de risico's van de verwerking aan de hand van onder meer de volgende punten:

* Het soort persoonsgegevens dat verwerkt wordt (normaal, bijzonder of gevoelig) en eventueel de daarbij behorende (risico)classificatie die de organisatie zelf aan de gegevens heeft gegeven. Gaat het bijvoorbeeld om een naam of een emailadres, wat minder gevoelige persoonsgegevens zijn, of gaat het om het verwerken van een BSN.

* De hoeveelheid betrokkenen van wie gegevens worden verwerkt. Hoe meer betrokkenen er zijn hoe meer eisen er worden gesteld aan de beveiliging van de gegevens.

* Het doel waarvoor gegevens worden verwerkt.

* De duur en de wijze waarop gegevens bewaard moeten worden. Er kan vervolgens onderscheid gemaakt worden tussen organisatorische beveiligingseisen, zoals het voorkomen van diefstal van een laptop met daarop persoonsgegevens uit de auto, en technische beveiligingseisen, zoals een uitgebreide IT omgeving die beveiligd wordt tegen virussen en waar encryptie van de gegevens wordt toegepast. Van een grote organisatie wordt meer verwacht ten aanzien van de te nemen beveiligingseisen.

Technische beveiligingsmaatregelen

☐ Up-to-date virusscan

☐ Beveiligde USB-sticks

☐ Accurate beveiliging medewerkerstelefoon

☐ Bitlocker toegangsmechanisme

☐ Unieke inlogcode en wachtwoord (regelmatig aanpassen)

☐ Versleutelde email

☐ Geen onbeveiligde externe harde schijven

☐ Geen onbeveiligde back ups maken

☐ Geen documenten op privé laptop op slaan

Organisatorische beveiligingsmaatregelen

☐ Clean desk policy

☐ Laptop niet onbemand achterlaten

☐ Laptop nooit achterlaten in de auto

☐ Privacy-screen(s) medewerkers

☐ Oude documenten op juiste manier vernietigen

☐ Zorgvuldig gebruik van USB-sticks

Bijlage 3: Proces rondom het melden van datalekken en de te verstrekken informatie

Wat is een beveiligingsincident en wanneer moet dit gemeld worden?

Een data-lek is een beveiligingsincident waarbij persoonsgegevens, die de verwerker namens de verwerkingsverantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Het gaat om gegevens die te koppelen zijn aan deze personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, log in gegevens, cookies, IP adressen of identificerende gegevens van computers of telefoons.

Hieronder vindt u een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- De website met logingegevens is gehackt of is toegankelijk voor derden.

- Verlies van een laptop of USB-stick met persoonsgegevens.

- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.

- Brieven of e-mails worden naar een verkeerd adres gestuurd.

- Een aanval van een hacker op het ICT systeem.

- Een verloren of gestolen telefoon waar persoonsgegevens op aanwezig zijn.

Wat te doen bij twijfel?

Als u op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stelt u zichzelf in ieder geval alvast de volgende vragen als hulpmiddel:

- Is er een technisch of fysiek beveiligingsprobleem?

- Gaat het probleem over de beveiliging van persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware, kunnen hieronder vallen.

- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteits)fraude mee kan worden gepleegd, zoals een burgerservicenummer.

- Zijn er grote hoeveelheden persoonsgegevens onbedoeld toegankelijk geworden voor derden?

- Gaat het om gegevens van kwetsbare groepen zoals kinderen?

- Worden de persoonsgegevens beheerd door een leverancier?

Wanneer u twijfelt, neem het zekere voor het onzekere en neem altijd contact op via **privacy@terborgse.nl**

Waar meldt u een beveiligingsincident?

Als u een beveiligingsincident hebt ontdekt, neemt u direct contact op met

Terborgse HandelsOnderneming BV, afdeling marketing en communicatie.

0315-325523 Of per e-mail: privacy@terborgse.nl

<u>Geef in uw e-mail beantwoording op de onderstaande vragen:</u>

De THO wil graag dat u onderstaande vragen beantwoordt. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt.

De afdeling marketing en communicatie kan u helpen met de beantwoording hiervan. Gaarne de vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. Geef een samenvatting van het beveiligingslek / beveiligingsincident / data-lek: wat is er gebeurd? *(Vermeld hier ook de naam van het betrokken systeem)*

2. Welke typen persoonsgegevens zijn betrokken bij het beveiligingsincident? *(Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven)*

3. Van hoeveel personen zijn de persoonsgegevens betrokken bij het beveiligingsincident? *(Geef a.u.b. een minimum en maximum aantal personen)*

4. Omschrijving groep personen om wiens gegevens het gaat. *(Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groep personen, zoals kinderen)*

5. Zijn de contactgegevens van de betrokken personen bekend? *(Het kan zijn dat betrokkenen geïnformeerd moeten worden over het data-lek, kunnen we deze personen in dat geval bereiken?)*

6. Wat is de oorzaak (root cause) van het beveiligingsincident? *(Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?)*

7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden? *(Geef dit a.u.b. zo specifiek mogelijk aan)*