PRIVACY COMPANY

Format Verwerkersovereenkomst

2020

Inhoudsopgave

Verwerkersovereenkomst Naam bedrijf

Datum: Datum

Contractpartijen:

1. Verwerkingsverantwoordelijke te weten Statutaire naam, statutair gevestigd te Plaats, vertegenwoordigd door naam en/of naam bestuurder

hierna te noemen: **'Verwerkingsverantwoordelijke'**,

en

2. Verwerker te weten Statutaire naam, statutair gevestigd te Plaats, vertegenwoordigd door naam en/of naam bestuurder

hierna te noemen: **'Verwerker'**,

gezamenlijk aan te duiden als: **'Partijen'**;

Overwegende dat:

Partijen hebben op Datum een Overeenkomst met betrekking tot Omschrijving gesloten. Ter uitvoering van deze Overeenkomst worden Persoonsgegevens verwerkt.

Verwerkingsverantwoordelijke hecht grote waarde aan het beschermen van deze Persoonsgegevens. Om die reden leggen Partijen in deze Verwerkersovereenkomst en de daarbij behorende bijlagen, te weten:

1. overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen
2. overzicht met beveiligingsmaatregelen
3. proces rondom het melden van Datalekken en de te verstrekken informatie met betrekking tot het Datalek vast wat Verwerker wel en niet mag doen met de Persoonsgegevens.

1. Definities

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

1.1. 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 identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

1.2. 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.

1.3. 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 ('Verwerkingsverantwoordelijke').

1.4. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke Persoonsgegevens verwerkt ('Verwerker').

1.5. Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte Persoonsgegeven betrekking hebben.

1.6. Verwerkersovereenkomst: deze Overeenkomst inclusief de bijlagen ('Verwerkersovereenkomst').

1.7. Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit.

1.8. 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 ('Datalek').

1.9. Gegevensbeschermingseffectbeoordeling: 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.

1.10. 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.

2. Totstandkoming, duur en beëindiging van deze Verwerkersovereenkomst

2.1. Deze Verwerkersovereenkomst treedt in werking op de datum waarop Partijen deze ondertekenen.

2.2. Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.

2.3. Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet apart worden opgezegd.

2.4. Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor Verwerker, zoals het melden van Datalekken waarbij Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn en de plicht tot geheimhouding blijven voortduren.

3. Verwerken Persoonsgegevens

3.1. Verwerker verwerkt alleen Persoonsgegevens in opdracht van Verwerkingsverantwoordelijke en Verwerker heeft geen zeggenschap over de Persoonsgegevens. Verwerker volgt instructies van Verwerkingsverantwoordelijke ten aanzien van de verwerking op en mag de Persoonsgegevens niet op een andere manier verwerken, tenzij Verwerkingsverantwoordelijke Verwerker daar van tevoren toestemming of opdracht voor geeft.

3.2. In Bijlage 1 wordt opgenomen welke Persoonsgegevens Verwerker precies zal verwerken en voor welke verwerkingsdoeleinden.

3.3. Verwerker houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.

3.4. Verwerker mag zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.

3.5. Wanneer Verwerker met toestemming van Verwerkingsverantwoordelijke andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.

3.6. Wanneer Verwerkingsverantwoordelijke een verzoek van een Betrokkene ontvangt ten aanzien van het uitoefenen van zijn of haar rechten, dan werkt Verwerker 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.

3.7. Rekening houdend met de aard van de verwerking en de ter beschikking staande informatie, verstrekt de Verwerker de Verwerkingsverantwoordelijke de benodigde informatie in het kader van het kunnen uitvoeren van een Gegevensbeschermingseffectbeoordeling door de Verwerkingsverantwoordelijke.

4. Beveiligen Persoonsgegevens

4.1. Verwerker zorgt ervoor dat de Persoonsgegevens voldoende worden beveiligd. Om verlies en onrechtmatige verwerkingen te voorkomen neemt Verwerker passende technische en organisatorische maatregelen.

4.2. Deze maatregelen zijn afgestemd op het risico van de Verwerking. Een overzicht van deze maatregelen en het beleid daaromtrent wordt opgenomen in Bijlage 2.

4.3. Ter controle van de genomen beveiligingsmaatregelen zal Verwerker aan Verwerkingsverantwoordelijke ieder jaar een rapportage sturen waarin de genomen beveiligingsmaatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor brengt Verwerker geen kosten in rekening aan Verwerkingsverantwoordelijke.

4.4. Verwerkingsverantwoordelijke mag een audit laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Verwerker verleent hierbij zijn medewerking. Waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.

4.5. De kosten voor de uitvoering van deze audit zullen voor rekening van Verwerker komen wanneer blijkt dat Verwerker zich niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.

4.6. De controle op de algehele verwerking van Persoonsgegevens door Verwerker kan, naast de auditmogelijkheid, ook geschieden via zelfevaluatie door Verwerker. Verwerker zal hierbij aan Verwerkingsverantwoordelijke een rapport verstrekken waarin Verwerker aantoont dat hij voldoet aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de organisatie van Verwerker.

4.7. Wanneer Partijen vinden dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Partijen in overleg over de wijziging daarvan. De kosten gemoeid met het wijzigen van de beveiligingsmaatregelen komen voor rekening van degene die de kosten maakt.

5. Exporteren Persoonsgegevens

5.1. Verwerker 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 Verwerkingsverantwoordelijke.

6. Geheimhouding

6.1. Verwerker zal de verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet kan.

6.2. Verwerker zorgt dat zijn/haar personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-) contracten op te nemen.

7. Datalekken

7.1. In geval van een ontdekking van een mogelijk Datalek zal Verwerker Verwerkingsverantwoordelijke hierover informeren binnen een termijn van 24 uur overeenkomstig het proces volgend uit Bijlage 3, zodat Verwerkingsverantwoordelijke indien nodig een melding van het Datalek bij de Toezichthouder kan doen.

7.2. Verwerker zal Verwerkingsverantwoordelijke op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek, ook zal Verwerker de getroffen maatregelen om het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, overleggen aan Verwerkingsverantwoordelijke.

7.3. Verwerker mag geen melding van een Datalek aan de Toezichthouder doen, wanneer bij het Datalek Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn. Ook mag Verwerker de Betrokkenen niet informeren over het Datalek. Deze verantwoordelijkheid ligt bij Verwerkingsverantwoordelijke.

7.4. Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

8. Aansprakelijkheid

8.1. Als Verwerker de verplichtingen uit deze Verwerkersovereenkomst niet nakomt, kan Verwerkingsverantwoordelijke Verwerker daarvoor aansprakelijk stellen.

8.2. Verwerker is aansprakelijk voor alle schade die Verwerkingsverantwoordelijke lijdt door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door de werkzaamheden van Verwerker.

8.3. *Indien Verwerker de verplichtingen in deze Verwerkersovereenkomst overtreedt, is Verwerker aan Verwerkingsverantwoordelijke een direct opeisbare boete verschuldigd van* Bedrag *voor iedere overtreding en* Bedrag *voor iedere dag dat Verwerker de overtreding begaat. Daarnaast behoudt Verwerkingsverantwoordelijke het recht om schadevergoeding te vorderen.* (optioneel)

8.4. Verwerker is aansprakelijk voor de aan Verwerkingsverantwoordelijke opgelegde bestuurlijke boete door de Toezichthouder als de schade het gevolg is van het onrechtmatig of nalatig handelen van Verwerker.

8.5. Verwerkingsverantwoordelijke is niet aansprakelijk voor aanspraken van Betrokkene of andere personen en organisaties waar Verwerker de samenwerking mee is aangegaan of waarvan Verwerker Persoonsgegevens verwerkt, als dit het gevolg is van het onrechtmatig of nalatig handelen van Verwerker.

9. Teruggave Persoonsgegevens en bewaartermijn

9.1. Na het beëindigen van deze Verwerkersovereenkomst geeft Verwerker de Persoonsgegevens terug aan Verwerkingsverantwoordelijke.

9.2. De overgebleven Persoonsgegevens zal Verwerker vernietigen na verstrijken van de wettelijke bewaartermijn en/of op verzoek van Verwerkingsverantwoordelijke. Hierbij valt bijvoorbeeld te denken aan Persoonsgegevens die om belastingtechnische redenen bewaard moeten blijven.

9.3. Verwerker zal na de teruggave en/of vernietiging van de Persoonsgegevens schriftelijk aan Verwerkingsverantwoordelijke verklaren niet langer in het bezit te zijn van de Persoonsgegevens.

10. Toepasselijk recht en geschillenbeslechting

10.1. De Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door het Nederlands recht.

10.2. Eventuele geschillen die tussen Partijen ontstaan, verband houdende met deze Verwerkersovereenkomst, worden voorgelegd aan de bevoegde rechter voor het arrondissement waarin de Verwerkingsverantwoordelijke gevestigd is.

11. 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 ten aanzien van de verwerking van Persoonsgegevens.

11.3. Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Partijen dit samen schriftelijk afspreken.

Aldus door Partijen overeengekomen en ondertekend:

Verwerkingsverantwoordelijke:

Ondertekend voor en namens Namens_____

Naam: Naam_____

Functie: Functie_____

Datum en plaats: Datum en plaats

Handtekening:

Verwerker:

Ondertekend voor en namens Naam_____

Naam: Naam_____

Functie: Functie_____

Datum en plaats: 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

Deel 1: Informatiebeveiligingsnorm

De Verwerker hanteert de volgende informatiebeveiligingsnorm (kruis aan wat van toepassing is):

☐ ISO 27001

☐ ISAE 3402

☐ Anders, namelijk _____

☐ Geen norm

De Verwerker toont aan dat het niveau van informatiebeveiliging toereikend is. De toereikendheid blijkt uit (kruis aan wat van toepassing is):

☐ Certificering / derden verklaring

Naam certificaat	**Organisatieonderdeel/ dienst waarop het certificaat betrekking heeft**	**Geldigheidsduur certificaat**	**Verklaring van toepasselijkheid**
			Indien aanwezig dient de Verwerker deze mee te sturen

☐ Anders, namelijk _____

☐ Geen aantoonbare toereikendheid.

Deel 2: Organisatorische en technische beveiligingsmaatregelen

De Verwerker heeft tenminste onderstaande beveiligingsmaatregelen getroffen (kruis aan wat van toepassing is):

Onderwerp	**Maatregel**	**Aanwezig**	**Niet aanwezig**	**Niet van toepassing**
Beleid	Informatiebe-veiligingsbeleid	☐	☐	☐
Veilig personeel	VOG	☐	☐	☐

	Awareness en training van personeel	☐	☐	☐
	Geheimhoudings-verklaring voor (ingehuurde) medewerkers	☐	☐	☐
Toegangsbeleid	Fysiek toegangsbeleid	☐	☐	☐
	Autorisatiebeleid	☐	☐	☐
	Wachtwoord-beleid	☐	☐	☐
	Twee factor authenticatie	☐	☐	☐
	Logging- en monitoringsbeleid	☐	☐	☐
Incident-management	Procedure beveiligingsincidenten en datalekken	☐	☐	☐
Continuïteit	Back-up en restore beleid	☐	☐	☐
	Business continuity plan	☐	☐	☐
Bedrijfsmiddelen	Beleid veilig gebruik maken van bedrijfsmiddelen en systemen	☐	☐	☐
Cryptografie (versleuteling)	Encryptie in transit	☐	☐	☐
	Encryptie at rest	☐	☐	☐
Informatie-systemen	Beleid aanschaf, ontwikkeling en onderhoud van informatie-systemen	☐	☐	☐
Onafhankelijke beoordelingen	Interne audit	☐	☐	☐
	Externe audit	☐	☐	☐
	Penetratie test	☐	☐	☐
	Vulnerability check	☐	☐	☐

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

Wat is een beveiligingsincident en wanneer moet dit gemeld worden?

Een datalek 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, login-gegevens, cookies, IP-adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- De website met login-gegevens 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 je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel je jezelf 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 (identiteit)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?

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met de _____.

Waar meld je het beveiligingsincident?

Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met de [invoeren naam contactpersoon of afdeling]:

Telefoon: _____

Of

E-mail: _____

Geef in je e-mail beantwoording op de onderstaande vragen

Wij willen graag dat je de onderstaande vragen voor ons beantwoordt. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt.

De [invoeren naam contactpersoon of afdeling] kan je helpen met de beantwoording hiervan. Gaarne de vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. Geef een samenvatting van het beveiligingslek/beveiligingsincident/datalek: 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 groepen personen, zoals kinderen.
5. Zijn de contactgegevens van de betrokken personen bekend? Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, 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.