Sjabloon verwerkersovereenkomst VVSG versie 2.0. (11/2024)

VERWERKERSOVEREENKOMST

[DATUM]

TUSSEN

[Entiteit] met maatschappelijke zetel gelegen te [adres] en met ondernemingsnummer [ondernemingsnummer], hierbij rechtsgeldig vertegenwoordigd door [naam en functie vertegenwoordiger], te bereiken via [VERMELDING VAN E-MAILADRES VERWERKINGSVERANTWOORDELIJKE];

Met als functionaris voor de gegevensbescherming, te bereiken via [VERMELDING VAN E-MAILADRES DPO]

Hierna: de “Verwerkingsverantwoordelijke”;

EN

[Onderneming] met maatschappelijke zetel gelegen te [adres] en met ondernemingsnummer [ondernemingsnummer], hierbij rechtsgeldig vertegenwoordigd door [naam en functie vertegenwoordiger], te bereiken via [VERMELDING VAN E-MAILADRES VERWERKER];

Met als functionaris voor de gegevensbescherming, te bereiken via [VERMELDING VAN E-MAILADRES]

Hierna: “de Verwerker”;

De Verwerkingsverantwoordelijke en de Verwerker worden hieronder ook wel gezamenlijk aangeduid als “de Partijen”;

NA TE HEBBEN UITEENGEZET

Op [datum / heden] hebben de Partijen een overeenkomst of meerdere overeenkomsten (opgesomd in bijlage 1) gesloten met betrekking tot [omschrijving dienstverleningsovereenkomst/raamovereenkomst], hierna genoemd de Opdracht;

In het kader van [deze overeenkomst/dit project] zal de Verwerker [ook] bepaalde Persoonsgegevens Verwerken in opdracht en voor rekening van de Verwerkingsverantwoordelijke. De Opdracht omvat ofwel:

* het leveren van toegang tot een product, website of andere waarbij de Verwerker alle controle over het platform behoudt en de Verwerkingsverantwoordelijke enkel als gebruiker optreedt. De dienst kan geleverd worden in een On Premise- of Cloud-omgeving;
* het uitvoeren van een opdracht waarbij de Verwerker instaat voor het verzamelen, beheer en gebruik van persoonsgegevens.

De partijen wensen nu hun afspraken met betrekking tot de uitvoering en organisatie van deze Verwerking van Persoonsgegevens te formaliseren in deze Verwerkersovereenkomst, die integraal deel uitmaakt van voornoemde dienstverleningsovereenkomst/raamovereenkomst.

WORDT OVEREENGEKOMEN WAT VOLGT

Artikel 1: Definities

Begrippen die in deze Verwerkersovereenkomst met hoofdletter worden gebruikt, moeten worden geïnterpreteerd zoals in dit artikel of elders in de Verwerkersovereenkomst gedefinieerd.

AVG

* Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);

Betrokkene

* De geïdentificeerde of identificeerbare natuurlijke persoon op wie een Persoonsgegeven betrekking heeft;

Datalek

* 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;

Derden

* Elke natuurlijke persoon, rechtspersoon, overheidsinstantie, dienst of ander orgaan andere dan de Betrokkene, de Verwerker, Subverwerker, de Verwerkingsverantwoordelijke en hun personeelsleden of aangestelden;

Opdracht

* De opdracht zoals omschreven in bijlage 1;

Persoonsgegevens

* Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals ook gedefinieerd in artikel 4, lid 1 van de AVG, die de Verwerker in het kader van de Opdracht Verwerkt;

Unierechtelijke of lidstaatrechtelijke bepaling

* Een bepaling opgelegd door Unierechtelijke of (EU) lidstaatrechtelijke wetgeving;

Verwerken / Verwerking

* Elke bewerking of 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, zoals ook gedefinieerd in artikel 4, lid 2 van de AVG;

Verwerkersovereenkomst

* Deze overeenkomst.

Artikel 2: Voorwerp (art. 28, lid 3 en 4 van de AVG)

2.1. De Verwerker Verwerkt Persoonsgegevens voor de Verwerkingsverantwoordelijke uitsluitend zoals omschreven in de Opdracht en overeenkomstig de in deze Overeenkomst vastgelegde verplichtingen. De Opdracht wordt nader omschreven in bijlage 1.

2.2. Elke Verwerking anders dan omschreven in de Opdracht is strikt verboden, met inbegrip van de doorgifte van Persoonsgegevens aan Derden, een derde land of een internationale organisatie, behoudens indien één van de hieronder opgesomde voorwaarden vervuld is:

* de Verwerkingsverantwoordelijke heeft schriftelijke instructies gegeven om bijkomende Verwerkingen uit te voeren; of
* een Unierechtelijke of lidstaatrechtelijke bepaling verplicht de Verwerker tot deze bijkomende Verwerking. De Verwerker zal de Verwerkingsverantwoordelijke desgevallend binnen een redelijke termijn voorafgaand aan de bijkomende Verwerking op de hoogte stellen van voornoemd wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Als de Verwerker een verzoek krijgt om Persoonsgegevens ter beschikking te stellen door een daartoe bevoegde instantie overeenkomstig een Unierechtelijke of lidstaatrechtelijke bepaling, beoordeelt zij eerst of het verzoek bindend is en of zij op grond van gedrags- en beroepsregels aan het verzoek moet voldoen. Als er geen strafrechtelijke of andere juridische belemmeringen zijn, dan stelt de Verwerker de Verwerkingsverantwoordelijke op de hoogte van het verzoek. De Verwerker doet dat binnen een termijn dat het voor de Verwerkingsverantwoordelijke mogelijk is om eventuele rechtsmiddelen tegen de verstrekking van de Persoonsgegevens in te stellen.

2.3. De Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk in kennis indien naar zijn mening een instructie inbreuk oplevert op de AVG of op andere Unierechtelijke of lidstaatrechtelijke bepalingen inzake gegevensbescherming.

Artikel 3: Duur (art. 28, lid 3,g van de AVG)

3.1. Deze overeenkomst loopt samen met de Opdracht beschreven in bijlage 1.

3.2. Artikels 5, 6, 7, 9, 10, 11 en 12 blijven van kracht na beëindiging van de Verwerkersovereenkomst.

Artikel 4: Beveiliging (art. 32 van de AVG)

4.1. De Verwerker treft alle passende technische en organisatorische beveiligingsmaatregelen die nodig zijn om de Persoonsgegevens te beveiligen, rekening houdend met de stand van de techniek en de kost voor beveiliging, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen. In het bijzonder zal de Verwerker de Persoonsgegevens beveiligen tegen vernietiging, verlies, vervalsing, niet toegelaten verspreiding of toegang en elke andere vorm van onwettige Verwerking. De minimale maatregelen die worden getroffen, worden door de Verwerker in bijlage 1 toegevoegd.

4.2. De Verwerker wijst een functionaris voor gegevensbescherming aan en heeft tenminste een actueel informatieveiligheidsbeleid en -plan.

Artikel 5: Vertrouwelijkheid (art. 29 van de AVG)

5.1. De Verwerker verbindt zich er uitdrukkelijk toe het vertrouwelijk karakter en de veiligheid van de Persoonsgegevens die hij in het kader van de Opdracht Verwerkt, te waarborgen.

5.2. De Verwerker maakt zich sterk dat alle personeelsleden of aangestelden die toegang hebben tot de Persoonsgegevens het vertrouwelijk karakter en de veiligheid van deze Persoonsgegevens zullen respecteren. De Verwerker zal erop toezien dat personeelsleden of aangestelden enkel toegang verkrijgen tot Persoonsgegevens nadat ze behoorlijk gebonden zijn door een wettelijke of contractuele vertrouwelijkheidsverplichting.

Artikel 6: Onderaanneming en subverwerkers (art. 28, lid 4 van de AVG)

6.1. Het is de Verwerker toegestaan andere verwerkers aan te stellen om Persoonsgegevens in het kader van de Opdracht te Verwerken (hierna: de “Subverwerker”). De Verwerkingsverantwoordelijke gaat akkoord met de lijst van Subverwerkers opgesomd in bijlage 1. Voor het aannemen van een andere Subverwerker licht de Verwerker de Verwerkingsverantwoordelijke binnen een redelijke termijn in over de toevoeging of verandering. De Verwerkingsverantwoordelijke kan vervolgens bezwaar maken tegen het aannemen van de voorgestelde Subverwerker.

6.2. In geval van bezwaar werken de partijen te goeder trouw samen om een (commercieel) redelijke wijziging door te voeren in de Opdracht waardoor beroep op de voorgestelde Subverwerker vermeden wordt; wanneer deze wijziging niet doorgevoerd kan worden binnen een termijn van 3 maanden na ontvangst van bezwaar door de Verwerker, kan de Verwerkingsverantwoordelijke deze verwerkersovereenkomst en de overeenkomst of overeenkomsten opgesomd in bijlage 1 met onmiddellijke ingang beëindigen door middel van een schriftelijke kennisgeving aan de Verwerker, voor zover zij betrekking heeft tot de diensten die beroep op de voorgestelde Subverwerker vereisen.

6.3. Extern ingehuurde medewerkers worden voor deze Verwerkersovereenkomst niet als Subverwerker beschouwd. De Verwerker zal erop toezien dat deze extern ingehuurde medewerkers dezelfde vertrouwelijkheidsclausule, zoals beschreven in artikel 5 van deze Verwerkersovereenkomst naleven zoals dit voor de eigen werknemers van de Verwerker het geval is.

6.4. De Verwerker en de Subverwerker sluiten een overeenkomst waarin dezelfde verplichtingen inzake gegevensbescherming opgelegd worden als dewelke in de voorliggende Verwerkersovereenkomst zijn opgenomen. De Verwerker zal de Subverwerkers ook dezelfde geheimhoudingsverplichting als deze die op haar rust opleggen middels een vertrouwelijkheidsovereenkomst. De Verwerker zal op eenvoudig verzoek van de Verwerkingsverantwoordelijke het nodige bewijs voorleggen om aan te tonen dat de overeenkomsten met haar Subverwerkers voldoen aan de in dit artikel gestelde voorwaarden.

6.5. De Verwerker houdt een actueel overzicht bij van de overeenkomsten met Subverwerkers en kan deze binnen redelijke termijn op eenvoudig verzoek bezorgen aan de Verwerkingsverantwoordelijke.

6.6. Indien een Subverwerker haar gegevensbeschermingsverplichtingen niet vervult, zal de Verwerker volledig aansprakelijk blijven ten opzichte van de Verwerkingsverantwoordelijke voor de naleving van deze verplichtingen.

Artikel 7: Bijstand (art. 28, lid 4, e-f van de AVG)

7.1. De Verwerker zal de Verwerkingsverantwoordelijke alle informatie verstrekken en alle bijstand verlenen die noodzakelijk is en/of die redelijkerwijze mag worden verwacht opdat de Verwerkingsverantwoordelijke in staat zou zijn om haar verplichtingen uit de AVG na te komen én van deze nakoming het bewijs te leveren.

De tijd en middelen die de Verwerker spendeert voor het verlenen van de bijstand eigen aan de verantwoordelijkheden van de Verwerker, zijn voor eigen rekening van de Verwerker.

7.2. De Verwerker verleent aan de Verwerkingsverantwoordelijke door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, bijstand bij het vervullen van diens plicht om verzoeken tot uitoefening van de in hoofdstuk III van de AVG vastgestelde rechten van de betrokkene, te beantwoorden.

Indien een Betrokkene zich rechtstreeks wendt tot de Verwerker om zich te beroepen op één van de rechten die hem ingevolge hoofdstuk III van de AVG zijn toegekend, zal de Verwerker dit onverwijld melden aan de Verwerkingsverantwoordelijke en alleen tegemoet komen aan het verzoek van de Betrokkene na schriftelijk akkoord van de Verwerkingsverantwoordelijke.

7.3. De Verwerker verbindt zich ertoe elk Datalek en alle ernstige pogingen tot onrechtmatige of ongeautoriseerde Verwerkingen of toegangen tot Persoonsgegevens zonder onredelijke vertraging, en uiterlijk 24 uur na kennisname, te melden aan de Verwerkingsverantwoordelijke conform artikel 33, lid 3 van de AVG aan de hand van het formulier in bijlage 2. Zelfs bij onvolledige informatie over het Datalek wordt de Verwerkingsverantwoordelijke verwittigd. De Verwerker zal alle maatregelen treffen die redelijkerwijs nodig zijn om (verdere) schending van de beveiligingsmaatregelen en eventuele schade te voorkomen of te beperken en zal aan de Verwerkingsverantwoordelijke alle informatie die zij nuttig of nodig acht, verschaffen.

Rekening houdend met de aard van de Verwerking en de hem ter beschikking staande informatie, verleent de Verwerker bovendien bijstand aan de Verwerkingsverantwoordelijke bij het nakomen van diens verplichtingen betreffende:

* het melden van een Datalek aan de toezichthoudende autoriteit conform artikel 33 van de AVG;
* het mededelen van een Datalek aan de betrokkene conform artikel 34 van de AVG.

Het is de Verwerker evenwel niet toegestaan om het Datalek zelf te melden aan de toezichthoudende autoriteit of de mededeling aan de betrokkene zelf te verrichten. Dit is uitsluitend de bevoegdheid van de Verwerkingsverantwoordelijke.

7.4. De Verwerker zal – rekening houdend met de aard van de Verwerking en de hem ter beschikking staande informatie – de Verwerkingsverantwoordelijke bijstand verlenen bij het nakomen van diens verplichtingen betreffende:

* het beveiligen van de verwerking conform artikel 32 van de AVG;
* het uitvoeren van een gegevensbeschermingseffectbeoordeling conform artikel 35 van de AVG;
* het voorafgaand aan een voorgenomen verwerking raadplegen van de toezichthoudende autoriteit, wanneer dit na een gegevensbeschermingseffectbeoordeling nodig zou blijken, conform artikel 36 van de AVG.

Artikel 8: Plaats van Verwerking (art. 3, art. 28, lid 3 van de AVG)

8.1. De Verwerker verwerkt de Persoonsgegevens alleen binnen de Europese Economische Ruimte, tenzij hierover met de Verwerkingsverantwoordelijke andere afspraken zijn gemaakt. Deze afspraken leggen de Partijen gezamenlijk schriftelijk vast op basis van artikel 46 van de AVG.

Artikel 9: Controle (art. 28, lid 3, h van de AVG)

9.1. De Verwerkingsverantwoordelijke of zijn daartoe aangestelde heeft op elk ogenblik het recht om de naleving van deze Verwerkersovereenkomst te controleren. Daartoe heeft zij het recht om zich ter plaatse te begeven in de lokalen of plaatsen waar de Verwerker de Verwerking uitvoert. De Verwerkingsverantwoordelijke zal de Verwerker minstens 10 dagen voorafgaand aan het uitvoeren van de controle schriftelijk inlichten. De Verwerkingsverantwoordelijke zal de controles, tenzij dwingend anders vereist, enkel op werkdagen tijdens kantooruren uitvoeren.

9.2. Op eenvoudig verzoek van de Verwerkingsverantwoordelijke is de Verwerker ertoe gehouden alle inlichtingen die van toepassing zijn bij de uitvoering van deze Verwerkersovereenkomst mee te delen en bijstand te verlenen bij het uitvoeren van de audits of bij het vervullen van de verplichting om verzoeken om uitoefening van de in de AVG vastgestelde rechten van de Betrokkene te beantwoorden. In audits geconstateerde tekortkomingen worden door de Verwerker opgepakt en omgezet tot een plan met corrigerende maatregelen. Dit plan wordt binnen een maand na vaststelling van de tekortkomingen ter beoordeling en goedkeuring aan Verwerkingsverantwoordelijke aangeboden. De Verwerker draagt voor eigen rekening zorg voor de implementatie van de corrigerende maatregelen en dit in overeenstemming met de timing die in het vooropgestelde plan (cfr. supra) is opgegeven, tenzij de partijen anders overeenkomen.

9.3. De kosten van de audit zijn ten laste van de Verwerkingsverantwoordelijke, tenzij blijkt dat de Verwerker niet voldeed aan de AVG en/of aan de voorwaarden van de Opdracht en/of deze Verwerkersovereenkomst.

Artikel 10: Aansprakelijkheid (art. 82, lid 2 van de AVG)

10.1. Artikel 82 van de AVG zet de aansprakelijkheid van Partijen ten aanzien van de Betrokkenen uiteen en bepaalt de eventuele aansprakelijkheidsverdeling en schadevergoedingsregeling tussen Partijen met betrekking tot de schade berokkend aan de Betrokkenen. Partijen beschouwen de inhoud en verplichtingen van artikel 82 van de AVG als integraal hernomen in de Verwerkersovereenkomst en zullen hier ook volledige uitvoering aan geven.

Artikel 11: Beëindiging (art. 28, lid 3, g van de AVG)

11.1. Indien de Verwerker zijn verplichtingen onder deze Verwerkersovereenkomst niet naleeft, kan de Verwerkingsverantwoordelijke, onverminderd het recht om een schadevergoeding te bekomen, na schriftelijke gemotiveerde ingebrekestelling de Opdracht geheel of gedeeltelijk beëindigen indien de Verwerker nalaat passende maatregelen te treffen.

11.2. Wanneer deze Verwerkersovereenkomst eindigt, bezorgt de Verwerker aan de Verwerkingsverantwoordelijke een actuele kopie van de Persoonsgegevens en van de databank(en) met de Persoonsgegevens die het resultaat zijn van de verwerking waarmee de Verwerker werd belast in een gestructureerd, gangbaar en machineleesbaar formaat. Deze overdracht gebeurt zonder onredelijke vertraging en zonder extra kosten en op een wijze die de Verwerkingsverantwoordelijke bepaalt.

11.3. Als alle Persoonsgegevens en databanken zijn doorgegeven, stelt de Verwerker onmiddellijk een einde aan elke verwerking van de Persoonsgegevens en vernietigt hij elke kopie en back-up van de Persoonsgegevens en databanken die hij nog zou bezitten zonder extra kosten voor de Verwerkingsverantwoordelijke en op een wijze die de Verwerkingsverantwoordelijke bepaalt, tenzij opslag van de Persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht.

11.4. De Verwerker dient na beëindiging van de Opdracht schriftelijk aan de Verwerkingsverantwoordelijke te bevestigen dat artikel 11.3 van deze overeenkomst werd uitgevoerd, dit binnen een redelijke termijn.

Artikel 12: Overige

12.1. Deze Verwerkersovereenkomst is onderworpen aan het Belgisch recht. Alle geschillen in verband met deze Verwerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter in het arrondissement waar de Verwerkingsverantwoordelijke gevestigd is.

12.2. Indien een bepaling in de Verwerkersovereenkomst geheel of gedeeltelijk ongeldig, onwettig of nietig zou worden verklaard, tast dit op geen enkele wijze de geldigheid, wettigheid en toepasbaarheid van de andere bepalingen aan. De Partijen zullen vervolgens te goeder trouw onderhandelen om de ongeldige, onwettige of nietige bepaling te vervangen door een geldige bepaling die zoveel als mogelijk de gevolgen heeft van de ongeldige, onwettige of nietige bepaling.

12.3. Aanvullingen en wijzigingen op deze Verwerkersovereenkomst dienen schriftelijk te gebeuren door middel van een addendum dat als bijlage aan deze Verwerkersovereenkomst zal worden gehecht.

Deze Verwerkersovereenkomst werd op \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[DATUM] te \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[PLAATS] opgesteld in evenveel exemplaren als er Partijen zijn. Aan elke Partij wordt één ondertekend exemplaar van de Verwerkersovereenkomst overhandigd.

Voor de Verwerkingsverantwoordelijke Voor de Verwerker

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[naam vertegenwoordiger], [naam vertegenwoordiger],

[Functietitel] [Functietitel]

BIJLAGEN

Bijlage 1: Omschrijving Opdracht, veiligheidsmaatregelen, lijst van Subverwerkers

Bijlage 2: Melden van een datalek

1. Bijlage 1 – Omschrijving van de Opdracht en vragenlijst Verwerker

*Vul onderstaande lijst aan. Voeg eventueel stavingsstukken toe als bijlage.*

* 1. De Opdracht

|  |  |
| --- | --- |
| Over welk product of welke dienst gaat het? |  |
| Is er sprake van het verwerken van persoonsgegevens? Zo neen, licht toe waarom er geen sprake is van verwerking van persoonsgegevens. Zo ja:   * Van hoeveel personen worden er gegevens verwerkt? * Vul de lijst aan onder 1.9. | * Neen: * Ja   Aantal personen: |
| Is het doel van de verwerking van persoonsgegevens binnen het project helder omschreven? Vul verder aan onder 1.9. | * Neen: * Ja: |
| Contactgegevens van de DPO, alsook een tweede contactpersoon in geval de DPO niet bereikbaar is. | DPO  Naam  Functie:  E-mailadres:  Telefoonnummer:  Tweede contactpersoon  Naam  Functie:  E-mailadres:  Telefoonnummer: |
| Heeft de verwerker een goedgekeurd informatieveiligheidsplan en -beleid? | * Neen: * Ja |
| Kan de verwerker aantonen dat hij voldoet aan een goedgekeurde gedragscode of certificatieschema waarmee kan worden aangetoond dat hij voldoende garanties heeft voor de verwerking van persoonsgegevens voor een verwerkingsverantwoordelijke?   * Bijvoorbeeld: certificaten zoals ISO27001. Indien ja, graag het bewijsmateriaal van certificatie in bijlage bezorgen. | * Neen: * Ja: |
| Is de documentatie inzake de geleverde dienst actueel en acuraat? | * Neen * Ja |
| De verwerkingsverantwoordelijke zal gestructureerd op de hoogte gebracht worden van eventuele wijzigingen van de geleverde dienst. | * Neen * Ja * N.v.t. |

* 1. Gegevens

|  |  |
| --- | --- |
| Zijn alle gegevens nodig om het doel te bereiken?   * Worden er zo weinig mogelijk gegevens verzameld? | * Neen * Ja * Neen * Ja |
| Kan het doel met geanonimiseerde of pseudo-anonieme gegevens worden bereikt (terwijl daar op dit moment geen gebruik van wordt gemaakt)? | * Neen * Ja |
| Kunnen de gegevens gebruikt worden om het gedrag, de aanwezigheid of prestaties van mensen in kaart te brengen en/of te beoordelen (ook al is dit niet het doel)?   * Denk hierbij bijvoorbeeld ook aan geolocatie, trackingsystemen, gebruik van metadata, etc. | * Neen * Ja: |
| Is het doel van het verzamelen van de gegevens publiekelijk bekend of kan het publiekelijk bekend gemaakt worden? | * Neen * Ja |
| De verwerker vertelt tegen de betrokkene dat de gegevens worden verzameld. | * Neen * Ja |
| * Zo neen: kunnen de betrokkenen op de hoogte zijn van het verzamelen van de gegevens? | * Neen * Ja * N.v.t. |
| * Zo ja: vertelt u tegen de betrokkene waarom de gegevens worden verzameld (wat u er mee gaat doen)? | * Neen * Ja * N.v.t. |

* 1. Organisatorische maatregelen (o.b.v. [vragenlijst informatieveiligheid verwerkers van de VTC)](https://www.vlaanderen.be/vlaamse-toezichtcommissie/verplichtingen-bij-het-verwerken-van-persoonsgegevens/verwerkersovereenkomst#vragenlijst-informatieveiligheid-verwerkers)

|  |  |
| --- | --- |
| **ISO 5.1** Is er een duidelijke security policy die alle domeinen van de ISO 27001/27002 afdekt – rekening houdende met beschreven “te beschouwen dimensies”? | * Neen: * Ja |
| **ISO 5.2** Zijn de rollen en verantwoordelijkheden vastgelegd met name in zake CISO, DPO, operationeel beheer, incidentenbeheer? | * Neen: * Ja: |
| **ISO 5.3** Is functiescheiding toegepast om ongeoorloofde acties onmogelijk te maken? | * Neen * Ja |
| **ISO 5.12/5.13** Wordt er een classificatie van data en van systemen toegepast? | * Neen * Ja |
| **ISO 5.16/5.17/5.18** Is er een strikt gebruikers- en toegangsbeheer? Met name voor geprivilegieerde beheerders? | * Neen * Ja |
| **ISO 5.19** Worden de contractuele verplichtingen 1-op-1 doorgezet naar de subverwerkers en houdt de verwerker daar minimaal jaarlijks toezicht op? | * Neen * Ja |
| **ISO 5.20** Worden alle belangrijke activiteiten (met name van beheerders) in onwijzigbare audit trails vastgelegd die toegankelijk zijn voor de verwerkings-verantwoordelijke? | * Neen * Ja |
| **ISO 5.21/5.22/5.23** De Verwerker kent duidelijke regels inzake levering en gebruik van software en hardware en (security) testing – toepasselijk voor elke wijziging. | * Neen * Ja |
| De verwerker voorziet al zijn systemen van de laatste updates. Beveiligingsupdates worden opgevolgd en geïnstalleerd volgens een patchmanagementproces. | * Neen * Ja |
| De verwerker voert anti-malwarecontroles uit om te helpen voorkomen dat kwaadaardige software ongeautoriseerde toegang tot klantgegevens krijgt. | * Neen * Ja |
| **ISO 5.24** Zijn er duidelijke systemen en processen voor het beheren (en coördineren) van veiligheidsincidenten? | * Neen * Ja |
| **ISO 5.34** Kent de verwerker de regels inzake privacybescherming en de bescherming van persoonsgegevens en past hij die toe? | * Neen * Ja |
| De vereisten voor de bescherming van gegevens en systemen worden geanalyseerd en gespecificeerd in samenwerking met de IT-leverancier(s) (subverwerkers). | * Neen * Ja |
| De verwerker houdt een register van beveiligingsinbreuken bij met een beschrijving van de inbreuk, het tijdstip, de gevolgen van de inbreuk, de naam van de melder en van degene aan wie de inbreuk werd gemeld. | * Neen * Ja |

* 1. Personele maatregelen (o.b.v. [vragenlijst informatieveiligheid verwerkers van de VTC](https://www.vlaanderen.be/vlaamse-toezichtcommissie/verplichtingen-bij-het-verwerken-van-persoonsgegevens/verwerkersovereenkomst#vragenlijst-informatieveiligheid-verwerkers))

|  |  |
| --- | --- |
| **ISO 6.1 / 6.2 /6.3** Zijn er duidelijke regels en is er toezicht op gedrag van geprivilegieerde beheerders?   * Worden veiligheidsregels jaarlijks herhaald in hun training? | * Neen * Ja * Neen * Ja |
| **ISO 6.4/6.5/6.6** Zijn er duidelijke regels in geval van non-compliant gedrag?   * Bij het veranderen van functie of verlaten van de firma? * Zijn alle medewerkers gebonden door een geheimhoudings-clausule? | * Neen * Ja * Neen * Ja * Neen * Ja |
| **ISO 6.7 / 6.8** Zijn er duidelijke regels inzake werken op afstand (enkel middels systemen van de verwerker)   * Zijn er duidelijke regels over het rapporteren van eventuele/mogelijke veiligheidsincidenten? | * Neen * Ja * Neen * Ja |

* 1. Fysieke maatregelen (o.b.v. [vragenlijst informatieveiligheid verwerkers van de VTC](https://www.vlaanderen.be/vlaamse-toezichtcommissie/verplichtingen-bij-het-verwerken-van-persoonsgegevens/verwerkersovereenkomst#vragenlijst-informatieveiligheid-verwerkers))

|  |  |
| --- | --- |
| **ISO 7.1/7.2/7.3/7.4** Zijn de toegang tot de systemen en de systemen die gebruikt worden bij beheer op niveau? | * Neen * Ja |
| **ISO 7.5/7.6/7.7/7.8/7.10/7.11** Zijn adequate maatregelen getroffen die ongeauthoriseerde toegang tot systemen en dragers van data in principe onmogelijk maken? | * Neen * Ja |

* 1. Technologische maatregelen (o.b.v. [vragenlijst informatieveiligheid verwerkers van de VTC](https://www.vlaanderen.be/vlaamse-toezichtcommissie/verplichtingen-bij-het-verwerken-van-persoonsgegevens/verwerkersovereenkomst#vragenlijst-informatieveiligheid-verwerkers))

|  |  |
| --- | --- |
| **ISO 8.1** Beschikken beheerders over adequate en beveiligde systemen? | * Neen * Ja |
| **ISO 8.2 / ISO 8.3 / ISO 8.4** Heeft de verwerker een aparte priviliged access management omgeving (PAM)?   * Wordt voor (beheers)toegang op afstand gebruik gemaakt van een VPN? * Is toegang beperkt tot een need-to-know? | * Neen * Ja * Neen * Ja * Neen * Ja |
| **ISO 8.5** Past de verwerker sterke authenticatie toe op alle processen en MFA voor alle geprivilegieerde toegangen? | * Neen * Ja |
| **ISO 8.7 / 8.8** Zijn de systemen maximaal beschermd tegen malware?   * Test de verwerker systemen adequaat tegen kwestbaarheden? | * Neen * Ja * Neen * Ja |
| **ISO 8.10 / 8.11 / 8.12 / 8.13** Beschermt de verwerker data adequaat en conform hun CIA-classificatie-niveaus? | * Neen * Ja |
| **ISO 8.14** Beschikt de verwerker conform de CIA-classificatie over de nodige back-up en disaster recovery systemen? | * Neen * Ja |
| **ISO 8.15/8.16** Beschikt de verwerker over adequate logging met inbegrip van welke gebruiker, tijd en activiteit en monitoring om security incidenten te kunnen detecteren? | * Neen * Ja |
| **ISO 8.20 / 8.21 / 8.22** Is de infrastructuur opgezet om data en systemen adequaat genoeg te scheiden? | * Neen * Ja |
| **ISO 8.24** Past de verwerker waar nodig adequate cryptografische maatregelen toe zoals signing of encryptie?  De verwerker maakt gebruikt van beveiligde verbindingen voor de toegang tot haar gegevens in het datacenter. Alle data die verzonden wordt over publieke netwerken gebeurt aan de hand van encryptie mechanismen.   * Zo ja, graag ook aanvullen welk encryptiemechanismen gebruikt worden. | * Neen * Ja * Neen * Ja |
| **ISO 8.25 / 8.26 / 8.27 / 8.28 / 8.29**  Heeft de verwerker een software delivery pipeline die elke code-/config-wijziging valideert op fouten/non-compliancies …? | * Neen * Ja |

* 1. Cloudoplossingen

|  |  |
| --- | --- |
| Gelet op [advies 2020/05 van de Vlaamse Toezichtcommissie](https://assets.vlaanderen.be/image/upload/v1691079697/VTC_A_2020_05_advies_qous2z.pdf) (p.10), in welke categorie (rood, oranje, groen) bevindt de gegevensverwerking door middel van de oplossing zich? Specifieer waarom. |  |
| (Indien vorige vraag oranje of rood): Gelet op advies [2020/05](https://assets.vlaanderen.be/image/upload/v1691079697/VTC_A_2020_05_advies_qous2z.pdf) en [2022/02](https://assets.vlaanderen.be/image/upload/v1691080875/VTC_A_2022_02_advies_K_icaaef.pdf) van de Vlaamse Toezichtcommissie, welke maatregelen neemt u om te persoonsgegevens te beveiligen om eventueel toezicht door buitenlandse overheidsinstanties te verhinderen? |  |

* 1. Externe partners en subverwerkers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Naam | Activiteit /  persoonsgegevens | Doel van de verwerking | Doorgiftemiddel conform AVG art. 45 – 47 (indien verwerkingslocatie buiten EER) | Genomen veiligheidsmaatregelen (indien van toepassing) |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |
| --- | --- |
| Worden de gegevens verkocht aan Derden?   * Zo ja, specifieer: | * Neen * Ja |

* 1. Gebruik persoonsgegevens

*Omschrijving van het doel van het gebruik van de persoonsgegevens: wat ga je doen en waarom wil je met die specifieke persoonsgegevens deze activiteit opzetten?*

Categorieën van persoonsgegevens

Klasse Generieke informatie benaming van het type persoonsinformatie

1 00 Er werden geen standaard datatypes gerelateerd aan persoonsgegevens, geïdentificeerd in de Informatieklasse 1 (Vertrouwelijkheidslabel: ‘Publiek’).

2 00 Professionele contact gegevens

3 00 Persoonlijke contactgegevens

3 01 Identificatie gegevens

3 02 Persoonlijke kenmerken

3 03 Consumptiegewoonten.

3 04 Woningkenmerken

3 05 Opleiding, ervaring en vorming

3 06 Beroep en betrekking

3 07 Vrijetijdsbesteding en interesses

3 08 Rijksregisternummer / Identificatienummer van de sociale zekerheid

4 00 Financiële en fiscale gegevens

4 01 Leefgewoonten

4 02 Fysieke, Medische of psychische gegevens en behandelingen

4 03 Samenstelling van het gezin

4 04 Juridische en gerechtelijke gegevens

4 05 Raciale of etnische gegevens

4 06 Gegevens over seksuele geaardheid

4 07 Politieke, filosofische of religieuze relaties en overtuigingen

4 08 Beeld- en geluidopnamen

4 09 Genetische en biometrische gegevens

4 10 Locatiegegevens

4 11 Contractuele detail met werkgever

4 12 Evaluatie en prestaties

4 13 Gegevens sociale zekerheid

4 14 Statuten en vergunningen

5 00 Er werden geen standaard datatypes gerelateerd aan persoonsgegevens, geïdentificeerd in de Informatieklasse 5 (Vertrouwelijkheidslabel: ‘zeer geheim’).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Klasse (zie hierboven) | Welk gegeven | Bewaartermijn |  | Doel van de verwerking |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

* 1. *[Optioneel:]* Dataflow

*Maak een schets van de flow van hoe gebruik van de data er zou kunnen uitzien. Hoe ga je de gegevens verzamelen? Waar ga je ze opslaan? Waarvoor ga je ze gebruiken? Met wie ga je ze delen? Wanneer kan je ze verwijderen?*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Verzamelen** | **Opslag** | **Gebruik** | **Delen** | **Verwijderen** |
| Betrokkene |  |  |  |  |  |
| Verwerker 1 |  |  |  |  |  |
| Subverwerker 1 |  |  |  |  |  |
| Subverwerker 2 |  |  |  |  |  |

1. Bijlage 2 – Melden van een datalek

*Indien niet alle informatie beschikbaar is, is het belangrijk om te melden wat reeds geweten is.*

|  |  |
| --- | --- |
| **Interne contactpersoon** | Naam:  E-mailadres:  Telefoonnummer: |
| **Bedrijf** | Naam:  Adres:  BTW-nummer: |
| **Datum** |  |
| **Wie heeft de inbreuk geconstateerd?** | Naam:  Functietitel: |
| **Wanneer is de inbreuk geconstateerd?** | Datum:  Tijd: |
| **Omschrijf het beveiligingsincident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan.** |  |
| **Wanneer heeft de inbreuk plaatsgevonden?** | 1. Op (datum en tijd) 2. Tussen (datum en tijd) en tussen (datum en tijd) 3. Nog niet vastgesteld 4. Er is sprake van een anonieme melding van een derde |
| **Classifcatie van de data:** | 1. Geen, de gegevens zijn niet herleidbaar tot een individu 2. Identificatiegegevens gegevens (naam, adres, …) 3. Telefoonnummers 4. E-mailadressen, Facebook ID’s, Twitter ID’s etc. 5. Gebruikersnamen, wachtwoorden of andere inloggegevens, klantnummers 6. Financiële gegevens: rekeningnummers, creditcardnummers 7. rijksregisternummer 8. Kopieën van identiteitsbewijzen 9. Demografische kenmerken (leeftijd, geslacht, nationaliteit, beroep, onderwijs) 10. Gegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid of lidmaatschap van een vakvereniging 11. Gegevens over iemands gezondheid of seksuele geaardheid 12. Strafrechtelijke persoonsgegevens of persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag 13. Gegevens over iemand financiële of economische situatie, gegevens over schulden, salaris- en betalingsgegevens 14. Afgeleide financiële data (inkomenscategorie, huizenbezit, autobezit) 15. Kenmerken m.b.t. levensstijl (o.a. gezinssamenstelling, woonsituatie, interesses, …) 16. Data verkregen uit (openbare) sociale profielen (Facebook-, LinkedIn- en Twitteraccounts, …) 17. Overig, namelijk: |
| **Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?** | A. Geen, de gegevens zijn niet herleidbaar tot een individu  B. Nog niet vastgesteld  C. Ten minste …………… (aantal), maar niet meer dan …………… (aantal) betrokkenen |
| **Omschrijf de groep mensen waarvan persoonsgegevens zijn betrokken bij de inbreuk:** |  |
| **Omstandigheden van het datalek?** | A. Alleen lezen (een niet geautoriseerde derde heeft (vertrouwelijke) data kunnen inzien. Verwerker heeft de data nog in zijn bezit.) - confidentialiteit is in gevaar  B. Kopiëren (een niet-geautoriseerde derde heeft data kunnen kopiëren. De data is ook nog in het bezit van Verwerker.) - confidentialiteit is in gevaar  C. Wijzigen (een niet-geautoriseerde derde heeft data (kunnen) wijzigen in systemen van Verwerker - Integriteit is in gevaar  D. Verwijderen of vernietigen (een niet-geautoriseerde derde heeft data verwijderd uit de systemen van Verwerker of data vernietigd.) - Beschikbaarheid is in gevaar  E. Diefstal - Beschikbaarheid is in gevaar  F. Nog niet bekend |
| **Zijn de Persoonsgegevens onbegrijpelijk of ontoegankelijk gemaakt voor ongeautoriseerde derden, bijvoorbeeld door encryptie en hashing?** | 1. Ja 2. Neen 3. Deels, namelijk: |
| **Zo ja, op welke manier zijn de Persoonsgegevens versleuteld:** |  |
| **Welke beveiligingsmaatregelen (technisch en organisatorisch) zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?** |  |

Dit sjabloon werd opgesteld in samenwerking met Interleuven, IOK, Polis, stad Hasselt, stad Mechelen, stad Oostende en VERA.