Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden

Benaming: ………………………………………………………………………………………………………………………

Adres/maatschappelijke zetel: ……………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………………………………………………………………

Inschrijvingsnummer bij de Kruispuntbank van Ondernemingen (KBO):…………………………………………………………………………………………………………………………………………

Vertegenwoordigd door: *[naam/voornaam van de persoon die gemachtigd is om de organisatie wettelijk te vertegenwoordigen]*

…………………………………………………………………………………………………………………………………………………..

Hierna de "organisatie" genoemd,

1. Toepassingsgebied van het beleid

Vanuit de bekommernis om het prestatievermogen en de beveiliging van onze netwerk- en informatiesystemen te verbeteren, hebben wij ervoor gekozen een beleid voor de gecoördineerde bekendmaking van kwetsbaarheden in te voeren. Zo kunnen deelnemers met goede bedoelingen mogelijke kwetsbaarheden in de systemen, uitrusting en producten van onze organisatie opsporen of ons elke ontdekte informatie over een kwetsbaarheid bezorgen.

De toegang tot onze informaticasystemen en -uitrusting wordt evenwel uitsluitend verleend met de bedoeling de beveiliging ervan te verbeteren en ons te informeren over bestaande kwetsbaarheden, met strikte inachtneming van de andere voorwaarden bepaald in dit document.

Ons beleid betreft beveiligingskwetsbaarheden die kunnen worden misbruikt door derden of die de goede werking van onze producten, diensten, netwerk- of informatiesystemen kunnen verstoren.

De deelnemer is eveneens gemachtigd om informaticagegevens in ons informaticasysteem in te voeren of dit te proberen, met inachtneming van de doeleinden en voorwaarden van dit beleid.

*[op te stellen lijst van de producten, diensten of websites binnen het toepassingsgebied]*

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

*[eventuele lijst van producten, diensten of websites buiten het toepassingsgebied]*

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

Systemen die afhankelijk zijn van derden vallen buiten het toepassingsgebied van dit beleid, behalve indien deze derden vooraf uitdrukkelijk verklaren akkoord te gaan met deze regels.

*[op te stellen lijst van systemen die worden gebruikt door de organisatie en afhankelijk zijn van derden en die niet onder het beleid vallen]*

- …………………………………………………………………………………………………………………………………………………

- …………………………………………………………………………………………………………………………………………………

Het onderzoek van de deelnemer met betrekking tot informatiesystemen die niet uitdrukkelijk onder dit beleid vallen, kan leiden tot de gerechtelijke vervolging van deze deelnemer.

1. Wederzijdse verplichtingen van de partijen
2. **Evenredigheid**

De deelnemer verbindt zich ertoe om bij al zijn activiteiten het evenredigheidsbeginsel nauwgezet na te leven, dat wil zeggen de beschikbaarheid van de door het systeem geleverde diensten niet te verstoren en geen gebruik te maken van de kwetsbaarheid buiten wat strikt noodzakelijk is voor het aantonen van het beveiligingsprobleem. Zijn houding moet evenredig blijven: indien het probleem op kleine schaal is aangetoond, moet niet verder worden gegaan.

Ons beleid heeft niet tot doel de opzettelijke kennisneming van de inhoud van informatica-, communicatie- of persoonsgegevens mogelijk te maken en een dergelijke kennisneming mag slechts toevallig plaatsvinden in het kader van het opsporen van kwetsbaarheden.

1. **Verboden acties**

De volgende acties zijn niet toegestaan voor de deelnemer:

- het kopiëren of wijzigen van gegevens van het informaticasysteem of het verwijderen van gegevens uit dat systeem;

- het wijzigen van de parameters van het informaticasysteem;

- de installatie van malware: virus, worm, Trojaans paard enz.;

- "denial of service"-aanvallen (Distributed Denial Of Service - DDOS);

- "social engineering"-aanvallen;

- phishing-aanvallen;

- aanvallen via ongewenste mails (spamming);

- diefstal van paswoorden of “brute force”-aanvallen;

- de installatie van een toestel dat het mogelijk maakt om niet voor het publiek toegankelijke communicatie of elektronische communicatie te onderscheppen, op te slaan of er kennis van te nemen;

- het met opzet onderscheppen, opslaan of kennisnemen van niet voor het publiek toegankelijke communicatie of van elektronische communicatie;

- het met opzet gebruiken, bijhouden, meedelen of verspreiden van de inhoud van niet voor het publiek toegankelijke communicatie of van gegevens van een informaticasysteem waarvan de deelnemer redelijkerwijze had moeten weten dat ze onwettig werden verkregen;

-………………………………………………………………………………………………………………………………………………………….

-………………………………………………………………………………………………………………………………………………………….

-………………………………………………………………………………………………………………………………………………………….

-………………………………………………………………………………………………………………………………………………………….

Indien de deelnemer hulp van een derde wenst om zijn onderzoek uit te voeren, dient hij zich ervan te vergewissen dat die derde vooraf kennisneemt van dit beleid en erin toestemt om, bij het verlenen van hulp, de voorwaarden van het beleid na te leven.

1. **Vertrouwelijkheid**

Zonder onze voorafgaande en uitdrukkelijke toestemming mag de deelnemer in geen geval informatie die hij heeft verzameld in het kader van ons beleid delen met derden of verspreiden onder derden.

Het is evenmin toegestaan informatica-, communicatie- of persoonsgegevens mee te delen aan derden of te verspreiden onder derden.

Indien de kwetsbaarheid ook andere organisaties in België kan treffen, kunnen de deelnemer of de verantwoordelijke organisatie dit niettemin melden aan het CCB (vulnerabilityreport@cert.be).

1. **Uitvoering te goeder trouw**

Onze organisatie verbindt zich ertoe dit beleid te goeder trouw uit te voeren en de deelnemer die de voorwaarden ervan naleeft noch burgerrechtelijk noch strafrechtelijk te vervolgen.

In hoofde van de deelnemer mag er geen sprake zijn van bedrieglijk opzet, het oogmerk om te schaden, of de wil om gebruik te maken van of schade te veroorzaken aan het bezochte systeem of aan de gegevens ervan. Dat geldt ook voor derde systemen in België of in het buitenland.

In geval van twijfel over bepaalde voorwaarden van ons beleid moet de deelnemer ons aanspreekpunt vooraf raadplegen en diens schriftelijke toestemming verkrijgen alvorens te handelen.

1. **Verwerking van persoonsgegevens**

Een CVDP heeft niet tot doel om intentioneel persoonsgegevens te verwerken. Het is echter wel mogelijk dat de deelnemer, zelfs toevallig, persoonsgegevens moet verwerken in het kader van zijn onderzoek naar kwetsbaarheden.

De verwerking van persoonsgegevens heeft een ruime betekenis en omvat met name het opslaan, wijzigen, opvragen, raadplegen, gebruiken of verstrekken van elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Het “identificeerbare” karakter van de persoon hangt niet af van de loutere wil tot identificatie van de gegevensverwerker, maar van de mogelijkheid om de persoon direct of indirect te identificeren aan de hand van deze gegevens (bijvoorbeeld: een e-mailadres, identificatienummer, online identificator, IP-adres of nog, locatiegegevens).

Zo is het mogelijk dat de deelnemer op beperkte wijze persoonsgegevens verwerkt. Bij het verwerken van dergelijke gegevens verbindt de deelnemer zich ertoe de wettelijke verplichtingen inzake de bescherming van persoonsgegevens[[1]](#footnote-1) en de voorwaarden van dit beleid na te leven, met name:

* De deelnemer verbindt zich ertoe persoonsgegevens enkel te verwerken volgens de instructies van onze organisatie, die in dit beleid bepaald zijn, en uitsluitend voor het opsporen van kwetsbaarheden in de systemen, uitrusting of producten van onze organisatie. Iedere verwerking van persoonsgegevens voor een ander doel is uitgesloten.
* De deelnemer verbindt zich ertoe de verwerking van persoonsgegevens te beperken tot wat noodzakelijk is voor het opsporen van kwetsbaarheden.
* De deelnemer waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden.
* De deelnemer neemt passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen (bijv. versleuteling). De deelnemer verklaart dat hij de risico’s in verband met de uitvoering van dit beleid begrijpt en dat hij de nodige expertise en ervaring heeft om de systemen, uitrusting en producten van onze organisatie in alle veiligheid en conform de toepasselijke wetten en regelgeving te testen.
* De deelnemer verbindt zich ertoe ons, voor zover mogelijk en rekening houdend met de aard van de verwerking en de informatie waarover hij beschikt, te helpen bij de uitvoering van onze verplichtingen inzake de uitoefening van de rechten van de betrokkenen, de beveiliging van de verwerking en iedere mogelijke impactanalyse.
* De deelnemer verbindt zich ertoe om ons zo snel mogelijk na kennisname van iedere mogelijke inbreuk in verband met persoonsgegevens[[2]](#footnote-2) hierover in te lichten op het adres [*in te vullen door de verantwoordelijke organisatie*].
* De deelnemer mag eventuele verwerkte persoonsgegevens niet langer bijhouden dan nodig is. Gedurende deze periode moet de deelnemer ervoor zorgen dat deze gegevens bijgehouden worden met waarborging van een op de risico’s afgestemd beveiligingsniveau (bij voorkeur versleuteld). Na afloop van de deelname aan het beleid moeten deze gegevens onmiddellijk verwijderd worden.
* De deelnemer verbindt zich ertoe een register bij te houden van de categorieën van verwerkingsactiviteiten die hij namens onze organisatie heeft uitgevoerd. Dit register bevat met name een beschrijving van de beveiligingsmaatregelen die hij heeft genomen, overeenkomstig artikel 30, § 2, van de AVG.

De deelnemer mag een beroep doen op een derde voor zijn onderzoek. Hij moet zich ervan vergewissen dat die derde vooraf kennisneemt van dit beleid en erin toestemt om, bij het verlenen van hulp, de voorwaarden van het beleid na te leven, met inbegrip van de vertrouwelijkheid en de uitvoering van passende beveiligingsmaatregelen. De deelnemer erkent dat hij volledig aansprakelijk blijft ten aanzien onze organisatie indien de derde op wie hij een beroep doet zijn verplichtingen inzake gegevensbescherming niet nakomt.

Indien de deelnemer persoonsgegevens die door onze organisatie worden opgeslagen en/of op enige andere wijze worden verwerkt, verwerkt op een manier die in strijd is met dit beleid of voor andere doeleinden dan het opsporen van mogelijke kwetsbaarheden in de systemen, producten en uitrusting van onze organisatie, erkent hij dat hij zal worden beschouwd als een verwerkingsverantwoordelijke en zal hij volledig aansprakelijk zijn voor de verwerking die hij uit dien hoofde heeft uitgevoerd.

*[optioneel:*

1. ***Toekenning van een beloning***

*Onze organisatie verbindt zich ertoe een beloning toe te kennen aan de deelnemer onder de volgende voorwaarden:*

*[deze beloning moet vooraf duidelijk zijn bepaald in dit beleid (naargelang het aantal, het belang of de kwaliteit van de verstrekte inlichtingen)]*

*……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………]*

Elk verzoek om een beloning buiten de door het CVDP bepaalde voorwaarden kan aldus worden gelijkgesteld met een illegale poging tot afpersing.]

1. Hoe beveiligingskwetsbaarheden melden?
2. **Aanspreekpunt**

U moet de ontdekte informatie uitsluitend naar het volgende e-mailadres sturen:

…………………………………………………………………………………………………………………………………………………………….

*[zoals bijvoorbeeld: vulnerabilitypolicy@(naam van de organisatie).be]*

*[optie: e-mailadres van een bug bounty-platform]*

en/of het volgende onlineformulier invullen: *[beveiligde URL in HTTPS]* …………………………………………………………………………………………………………………………………………………………….

*[optie en/of u inschrijven op het volgende bug bounty-platform: [URL] ……………………………………………………………………………………………………………………………………………………………]*

Wij verzoeken u voor zover mogelijk de volgende beveiligde communicatiemiddelen te gebruiken:

…………………………………………………………………………………………………………………………………………………………….

*[beveiligde overdracht die bijvoorbeeld gebruik maakt van Transport Layer Security (TLS) of de voorganger ervan Secure Sockets Layer (SSL) , Secure Multipurpose Internet Mail Extensions (S/MIME) of Pretty Good Privacy (PGP) met de volgende Key ID ……………………………………………………………………..]*

U kunt eveneens contact opnemen met de dienst of de persoon die verantwoordelijk is voor het beleid, op het (de) volgende telefoonnummer(s):

…………………………………………………………………………………………………………………………………………………………….

1. **Te bezorgen informatie**

Stuur ons zo snel mogelijk na uw ontdekking de hieraan verbonden informatie met behulp van: [*het formulier in bijlage I] of [het onlineformulier dat u hier vindt (URL)]*.

1. Procedure
2. **Ontdekking**

Wanneer een deelnemer informatie over een mogelijke kwetsbaarheid ontdekt, moet hij voor zover mogelijk vooraf controles uitvoeren om het bestaan van de kwetsbaarheid te bevestigen en eventuele risico’s te identificeren.

1. **Melding**

De deelnemer verbindt zich ertoe om de technische informatie over de mogelijke kwetsbaarheden zo snel mogelijk te bezorgen aan het aanspreekpunt [of aan de coördinator (optioneel)] vermeld in punt 3 a) van dit beleid, met behulp van de vermelde beveiligde communicatiemiddelen.

Onze organisatie verbindt zich ertoe om, wanneer ze een melding ontvangt, de deelnemer zo snel mogelijk een bericht van ontvangst te sturen [met, indien mogelijk, de interne referentie ervan, een herinnering aan de voornaamste verplichtingen van het CVDP] en de volgende stappen van de procedure.

1. **Communicatie**

De partijen verbinden zich ertoe alles in het werk te stellen om een permanente en doeltreffende communicatie te garanderen. De door de deelnemer verstrekte inlichtingen kunnen immers heel nuttig zijn om de kwetsbaarheid te identificeren en er een oplossing voor te vinden.

Indien na een redelijke termijn een reactie van een van de partijen van het CVDP uitblijft, kunnen de partijen een beroep doen op het Centrum voor Cybersecurity België (CCB) (vulnerabilityreport@cert.be) als (standaard-) coördinator.

1. **Onderzoek**

Tijdens de onderzoeksfase zal onze organisatie de omgeving en de gesignaleerde handelwijze reproduceren om de meegedeelde informatie te controleren.

Onze organisatie verbindt zich ertoe om de deelnemer regelmatig op de hoogte te houden van de resultaten van het onderzoek en van het gevolg dat aan zijn melding wordt gegeven.

Tijdens deze procedure zullen de partijen ervoor zorgen dat ze de link leggen met gelijkaardige of aanverwante meldingen, dat ze het risico en de ernst van de kwetsbaarheid beoordelen en dat ze eventuele andere getroffen producten of systemen identificeren.

1. **Ontwikkeling van een oplossing**

Het bekendmakingsbeleid heeft tot doel de ontwikkeling van een oplossing mogelijk te maken om de kwetsbaarheid van het informaticasysteem weg te werken vooraleer schade wordt aangericht.

Rekening houdend met de stand van de techniek, de uitvoeringskosten, de ernst van de risico’s voor de gebruikers en de technische beperkingen zal onze organisatie proberen om uiterlijk binnen de 90 kalenderdagen een oplossing te ontwikkelen.

In deze fase verbinden onze organisatie en haar partners zich ertoe enerzijds positieve testen uit te voeren om na te gaan of de oplossing correct werkt en anderzijds negatieve testen om er zeker van te zijn dat de oplossing de goede werking van de andere bestaande functionaliteiten niet verstoort.

1. **Eventuele openbare bekendmaking**

Onze organisatie zal, in overleg met de deelnemer, beslissen op welke wijze het bestaan van de kwetsbaarheid eventueel openbaar wordt gemaakt. Deze openbare bekendmaking mag ten vroegste tegelijk met de toepassing van een oplossing en de verspreiding van een beveiligingsbericht voor de gebruikers plaatsvinden.

Indien een kwetsbaarheid ook andere organisaties treft, moet de verantwoordelijke organisatie dit in ieder geval melden aan het Centrum voor Cybersecurity België (vulnerabilityreport@cert.be), zelfs als ze niet wil dat de kwetsbaarheid openbaar wordt gemaakt.

Onze organisatie verbindt zich er eveneens toe opmerkingen van gebruikers over de toepassing van de oplossing te verzamelen en de nodige corrigerende maatregelen te nemen om eventuele problemen veroorzaakt door de oplossing te regelen, onder meer inzake compatibiliteit met andere producten of diensten.

1. Toepasselijk recht

Het Belgisch recht is van toepassing op geschillen in verband met de uitvoering van dit beleid.

[Optioneel:

Het CCB (vulnerabilityreport@cert.be) kan optreden als bemiddelaar tussen onze organisatie en de deelnemer voor problemen in verband met de toepassing van dit beleid.]

1. Duur

De regels van het beleid zijn toepasselijk vanaf xx/xx/xxxx tot ze eventueel worden gewijzigd of opgeheven door onze organisatie. Deze wijzigingen of opheffingen worden bekendgemaakt op de website van onze organisatie en zijn automatisch van toepassing 30 dagen na de bekendmaking ervan.

Datum,

Plaats,

Handtekening, [persoon gemachtigd om de organisatie wettelijk te vertegenwoordigen]

**Bijlage I: Formulier voor de melding van kwetsbaarheden**

Bezorg ons voldoende informatie zodat wij het probleem kunnen reproduceren en het zo snel mogelijk kunnen oplossen.

Wij verzoeken u om ons ten minste de volgende relevante informatie te bezorgen:

|  |  |
| --- | --- |
| Naam:Voornaam: |  |
| (Adres/Land): |  |
| E-mailadres:Telefoonnummer:  |  |
| Beschrijving van de kwetsbaarheid: |  |
| Soort kwetsbaarheid: |  |
| Configuratiedetails: |  |
| Besturingssysteem: |  |
| Uitgevoerde bewerkingen (logs): |  |
| Gebruikte tools: |  |
| Data en tijdstippen van de tests: |  |
| IP-adres of URL van het getroffen systeem: |  |
| Indien persoonsgegevens worden verwerkt: | * Soorten geraadpleegde/verwerkte persoonsgegevens:
* Categorieën van betrokkenen (klant, werknemer, leverancier):
* Doorgifte van gegevens aan/toegang vanuit een land buiten de Europese Unie of de Europese Economische Ruimte?

Zo ja: * vermeld het (de) betrokken land(en):
* stuur de ingevulde en ondertekende bijlage II terug.
 |
| Iedere andere relevante informatie: |  |
| Bijlagen (screenshots). |  |

**Wat doen wij met uw persoonsgegevens?**

Wij verzoeken u ons beleid voor de bescherming van persoonsgegevens te lezen op *[link of e-mailadres in te vullen door de organisatie]*. *[Indien nodig vermeldt de organisatie hieronder de specifieke kenmerken of afwijkingen die van toepassing zijn op de verwerking van persoonsgegevens van hackers ten opzichte van haar “algemene” gegevensbeschermingsbeleid].*

**Bijlage II – Doorgifte van persoonsgegevens door de deelnemer in een land buiten de Europese Unie of de Europese Economische Ruimte.**

**Modelcontractbepalingen inzake gegevensbescherming (nr. 2010/87/EU)**

Voor de toepassing van artikel 26, lid 2, van Richtlijn 95/46/EG voor de doorgifte van persoonsgegevens aan verwerkers die gevestigd zijn in derde landen die geen passend gegevensbeschermingsniveau waarborgen.

Naam van de organisatie die de gegevens uitvoert (de verantwoordelijke organisatie)

 (hierna de “gegevens**exporteur**”genoemd)

enerzijds, en

Naam van de organisatie die de gegevens invoert (de deelnemer)

(hierna de “gegevens**importeur”** genoemd)

anderzijds, hierna elk afzonderlijk “partij” en gezamenlijk “de partijen” genoemd,

ZIJN OVEREENGEKOMEN de volgende contractbepalingen (hierna “de bepalingen” genoemd) vast te stellen teneinde passende waarborgen te bieden ten aanzien van de bescherming van de persoonlijke levenssfeer en de fundamentele rechten en vrijheden van personen bij de doorgifte van de in aanhangsel 1 vermelde persoonsgegevens door de gegevensexporteur aan de gegevensimporteur.

***Bepaling 1***

**Definities**

Voor de toepassing van de bepalingen:

|  |  |
| --- | --- |
| a) |  gelden voor “persoonsgegevens”, “bijzondere categorieën gegevens”, “verwerken/verwerking”, “voor de verwerking verantwoordelijke”, “verwerker”, “betrokkene” en “toezichthoudende autoriteit” dezelfde definities als in Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens[(1)](https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32010D0087&from=NL#ntr1-L_2010039FR.01001001-E0001); |

|  |  |
| --- | --- |
| b) |  wordt onder “gegevensexporteur” verstaan: de voor de verwerking verantwoordelijke die de persoonsgegevens doorgeeft; |

|  |  |
| --- | --- |
| c) |  wordt onder “gegevensimporteur” verstaan: de verwerker die overeenkomt van de gegevensexporteur persoonsgegevens te ontvangen om deze na doorgifte namens de gegevensexporteur te verwerken in overeenstemming met zijn instructies en de voorwaarden van deze bepalingen, en die niet onderworpen is aan een regeling van een derde land die passende bescherming biedt in de zin van artikel 25, lid 1, van Richtlijn 95/46/EG; |

|  |  |
| --- | --- |
| d) |  wordt onder “subverwerker” verstaan: een verwerker die door de gegevensimporteur of een andere voor de gegevensimporteur werkende subverwerker is gecontracteerd en die overeenkomt van de gegevensimporteur of van een andere voor de gegevensimporteur werkende subverwerker persoonsgegevens te ontvangen, uitsluitend ten behoeve van de verwerkingsactiviteiten die namens de gegevensexporteur worden verricht na de doorgifte, overeenkomstig de instructies van de gegevensexporteur, de voorwaarden van deze bepalingen en de voorwaarden van het schriftelijke contract inzake subverwerking; |

|  |  |
| --- | --- |
| e) |  wordt onder “toepasselijk recht inzake gegevensbescherming” verstaan: de wettelijke bepalingen ter bescherming van de fundamentele rechten en vrijheden van personen, en met name hun recht op bescherming van de persoonlijke levenssfeer in verband met de verwerking van persoonsgegevens, die in de lidstaat van vestiging van de gegevensexporteur van toepassing zijn op een voor de verwerking verantwoordelijke; |

|  |  |
| --- | --- |
| f) |  wordt onder “technische en organisatorische beveiligingsmaatregelen” verstaan: maatregelen die tot doel hebben persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking de doorzending van gegevens in een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking. |

***Bepaling 2***

**Bijzonderheden betreffende de doorgifte**

De bijzonderheden betreffende de doorgifte, met name, in voorkomend geval, de bijzondere categorieën persoonsgegevens, worden nader omschreven in aanhangsel 1, dat integraal deel uitmaakt van deze bepalingen.

***Bepaling 3***

**Derdenbeding**

|  |  |
| --- | --- |
| 1. |  De betrokkene kan deze bepaling en bepaling 4, onder b) tot en met i), bepaling 5, onder a) tot en met e) en g) tot en met j), bepaling 6, leden 1 en 2, bepaling 7, bepaling 8, lid 2, en de bepalingen 9 tot en met 12 als derde begunstigde tegenover de gegevensexporteur afdwingen. |

|  |  |
| --- | --- |
| 2. |  De betrokkene kan deze bepaling, bepaling 5, onder a) tot en met e) en onder g), bepaling 6, bepaling 7, bepaling 8, lid 2, en de bepalingen 9 tot en met 12 tegenover de gegevensimporteur afdwingen ingeval de gegevensexporteur feitelijk is verdwenen of heeft opgehouden rechtens te bestaan, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur heeft overgenomen en daardoor de rechten en verplichtingen van de gegevensexporteur op zich neemt; in dit geval kan de betrokkene de genoemde bepalingen tegenover deze rechtsopvolger afdwingen. |

|  |  |
| --- | --- |
| 3. |  De betrokkene kan deze bepaling, bepaling 5, onder a) tot en met e) en onder g), bepaling 6, bepaling 7, bepaling 8, lid 2, en de bepalingen 9 tot en met 12 tegenover de subverwerker afdwingen ingeval zowel de gegevensexporteur als de gegevensimporteur feitelijk is verdwenen, heeft opgehouden rechtens te bestaan of insolvent is geworden, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur heeft overgenomen en daardoor de rechten en verplichtingen van de gegevensexporteur op zich neemt; in dat geval kan de betrokkene de genoemde bepalingen tegenover deze rechtsopvolger afdwingen. Deze burgerlijke aansprakelijkheid van de subverwerker blijft beperkt tot de verwerkingsactiviteiten die deze zelf heeft uitgevoerd overeenkomstig deze bepalingen. |

|  |  |
| --- | --- |
| 4. |  De partijen verzetten zich er niet tegen dat de betrokkene door een vereniging of andere instelling wordt vertegenwoordigd, indien de betrokkene dit uitdrukkelijk wenst en dit in het nationale recht is toegestaan. |

***Bepaling 4***

**Verplichtingen van de gegevensexporteur**

De gegevensexporteur stemt ermee in en garandeert dat:

|  |  |
| --- | --- |
| a) |  de verwerking van de persoonsgegevens, met inbegrip van de doorgifte zelf, is gebeurd en zal blijven gebeuren in overeenstemming met alle relevante bepalingen van het toepasselijke recht inzake gegevensbescherming (en, in voorkomend geval, is gemeld aan de bevoegde autoriteiten van de lidstaat waar de gegevensexporteur is gevestigd), en dat zij niet in strijd is met de toepasselijke bepalingen van die staat; |

|  |  |
| --- | --- |
| b) |  hij de gegevensimporteur heeft opgedragen, en gedurende de verwerking van de persoonsgegevens zal opdragen, de persoonsgegevens uitsluitend namens de gegevensexporteur en in overeenstemming met het toepasselijke recht inzake gegevensbescherming en deze bepalingen te verwerken; |

|  |  |
| --- | --- |
| c) |  hij de gegevensimporteur voldoende waarborgen zal bieden ten aanzien van de technische en organisatorische beveiligingsmaatregelen die in aanhangsel 2 bij dit contract worden omschreven; |

|  |  |
| --- | --- |
| d) |  deze beveiligingsmaatregelen, na een beoordeling van de vereisten van het toepasselijke recht inzake gegevensbescherming, geschikt zijn bevonden om persoonsgegevens te beschermen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang, met name wanneer de verwerking doorzending van gegevens via een netwerk omvat, dan wel tegen enige andere vorm van onwettige verwerking, en dat deze maatregelen gezien de aan de verwerking en de aard van de te beschermen gegevens verbonden risico’s een passend beveiligingsniveau waarborgen, gelet op de stand van de techniek en de kosten van de tenuitvoerlegging; |

|  |  |
| --- | --- |
| e) | hij op de naleving van deze beveiligingsmaatregelen zal toezien; |

|  |  |
| --- | --- |
| f) |  wanneer de doorgifte bijzondere categorieën gegevens betreft, de betrokkene ervan in kennis is gesteld, of vóór of zo spoedig mogelijk na de doorgifte ervan in kennis zal worden gesteld, dat zijn gegevens kunnen worden doorgegeven naar een derde land dat geen passende bescherming biedt als bedoeld in Richtlijn 95/46/EG; |

|  |  |
| --- | --- |
| g) |  hij overeenkomstig bepaling 5, onder b), en bepaling 8, lid 3, ontvangen kennisgevingen van de gegevensimporteur of een subverwerker aan de toezichthoudende autoriteit zal doorzenden, wanneer hij (dat wil zeggen de gegevensexporteur) besluit de doorgifte voort te zetten of de opschorting ervan op te heffen; |

|  |  |
| --- | --- |
| h) |  hij op verzoek een afschrift van deze bepalingen ter beschikking van de betrokkenen zal stellen, met uitzondering van aanhangsel 2, alsook een beknopte beschrijving van de beveiligingsmaatregelen en een afschrift van elk contract voor subverwerkingsdiensten dat overeenkomstig deze bepalingen dient te worden opgesteld; indien de bepalingen of het contract commerciële informatie bevatten, mag de gegevensexporteur deze commerciële informatie verwijderen; |

|  |  |
| --- | --- |
| i) | in geval van subverwerking de verwerkingsactiviteiten worden uitgevoerd overeenkomstig bepaling 11 door een subverwerker die ten minste hetzelfde beschermingsniveau voor de persoonsgegevens en de rechten van de betrokkene waarborgt als de gegevensimporteur overeenkomstig deze bepalingen; en |

|  |  |
| --- | --- |
| j) | hij zal toezien op de naleving van bepaling 4, onder a) tot en met i). |

***Bepaling 5***

**Verplichtingen van de gegevensimporteur**

De gegevensimporteur stemt ermee in en garandeert dat:

|  |  |
| --- | --- |
| a) |  hij de persoonsgegevens uitsluitend namens de gegevensexporteur en in overeenstemming met diens instructies en met deze bepalingen verwerkt; indien hij om welke reden dan ook daartoe niet in staat is, stemt hij ermee in de gegevensexporteur onverwijld daarvan in kennis te stellen, in welk geval de gegevensexporteur de gegevensdoorgifte mag opschorten en/of het contract mag beëindigen; |

|  |  |
| --- | --- |
| b) |  hij geen reden heeft aan te nemen dat de op hem toepasselijke wetgeving hem belet de van de gegevensexporteur ontvangen instructies en zijn verplichtingen uit hoofde van het contract na te komen, en dat hij in geval van een wijziging in deze wetgeving die in aanzienlijke mate afbreuk dreigt te doen aan de in de bepalingen opgenomen waarborgen en verplichtingen, de gegevensexporteur, zodra hij de wijziging kent, onverwijld daarvan in kennis stelt, in welk geval de gegevensexporteur de gegevensdoorgifte mag opschorten en/of het contract mag beëindigen; |

|  |  |
| --- | --- |
| c) |  hij de in aanhangsel 2 omschreven technische en organisatorische beveiligingsmaatregelen vóór de verwerking van de doorgegeven persoonsgegevens heeft getroffen; |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| d) |  hij de gegevensexporteur onverwijld ervan in kennis stelt wanneer:

|  |  |
| --- | --- |
| i) |  een wetshandhavingsinstantie een juridisch bindend verzoek om verstrekking van persoonsgegevens heeft gedaan, tenzij deze kennisgeving anderszins is verboden, zoals een strafrechtelijk verbod dat tot doel heeft de vertrouwelijkheid van een politioneel onderzoek te bewaren; |

|  |  |
| --- | --- |
| ii) |  iemand per ongeluk of op ongeoorloofde wijze toegang tot de gegevens heeft gehad; en |

|  |  |
| --- | --- |
| iii) |  hij van de betrokkenen rechtstreeks een verzoek heeft ontvangen, waarop hij niet ingaat, tenzij hem dit anderszins is toegestaan; |

 |

|  |  |
| --- | --- |
| e) |  hij alle vragen van de gegevensexporteur betreffende de door hem uitgevoerde verwerking van de doorgegeven persoonsgegevens spoedig naar behoren beantwoordt en het advies van de toezichthoudende autoriteit volgt bij de verwerking van de doorgegeven gegevens; |

|  |  |
| --- | --- |
| f) |  hij op verzoek van de gegevensexporteur zijn verwerkingsvoorzieningen beschikbaar stelt voor controle van de onder deze bepalingen vallende verwerkingsactiviteiten, die wordt uitgevoerd door de gegevensexporteur of door een controleorgaan waarvan de leden onafhankelijk zijn, over de vereiste beroepskwalificaties beschikken, tot geheimhouding verplicht zijn en door de gegevensexporteur worden aangewezen, in voorkomend geval, in overleg met de toezichthoudende autoriteit; |

|  |  |
| --- | --- |
| g) |  hij, wanneer de betrokkene geen afschrift van de gegevensexporteur kan verkrijgen, hem op verzoek een afschrift van deze bepalingen alsook eventuele subverwerkingscontracten ter beschikking stelt, met uitzondering van aanhangsel 2 dat door een beknopte beschrijving van de beveiligingsmaatregelen wordt vervangen; indien de bepalingen of contracten commerciële informatie bevatten, mag de gegevensimporteur deze commerciële informatie verwijderen; |

|  |  |
| --- | --- |
| h) |  hij, wanneer subverwerking plaatsvindt, de gegevensexporteur tevoren heeft ingelicht en diens schriftelijke toestemming heeft verkregen; |

|  |  |
| --- | --- |
| i) |  de verwerkingsdiensten van de subverwerker overeenkomstig bepaling 11 zullen worden uitgevoerd; |

|  |  |
| --- | --- |
| j) |  hij van elk subverwerkingscontract dat hij in het kader van deze bepalingen aangaat, onverwijld een afschrift verstuurt naar de gegevensexporteur. |

***Bepaling 6***

**Aansprakelijkheid**

|  |  |
| --- | --- |
| 1. |  De partijen komen overeen dat elke betrokkene die ten gevolge van een schending van de verplichtingen bedoeld in bepaling 3 of bepaling 11 door een partij of een subverwerker schade heeft geleden, het recht heeft van de gegevensexporteur een vergoeding voor de geleden schade te ontvangen. |

|  |  |
| --- | --- |
| 2. | Wanneer de betrokkene geen vordering tot schadevergoeding wegens niet-nakoming door de gegevensimporteur of diens subverwerker van een van de in bepaling 3 of bepaling 11 bedoelde verplichtingen, als bedoeld in lid 1, tegen de gegevensexporteur kan instellen doordat de gegevensexporteur feitelijk is verdwenen, heeft opgehouden rechtens te bestaan of insolvent is geworden, stemt de gegevensimporteur ermee in dat de betrokkene een vordering kan instellen tegen de gegevensimporteur alsof hij de gegevensexporteur was, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur heeft overgenomen, in welk geval de betrokkene zijn rechten tegenover die rechtsopvolger kan doen gelden.De gegevensimporteur kan zich niet aan zijn aansprakelijkheid onttrekken door zich te beroepen op de niet-nakoming van verplichtingen door de subverwerker. |

|  |  |
| --- | --- |
| 3. |  Wanneer de betrokkene de in lid 1 of 2 bedoelde vordering wegens niet-nakoming door de subverwerker van een van de in bepaling 3 of bepaling 11 bedoelde verplichtingen niet tegen de gegevensexporteur of de gegevensimporteur kan instellen doordat zowel de gegevensexporteur als de gegevensimporteur feitelijk is verdwenen, heeft opgehouden rechtens te bestaan of insolvent is geworden, stemt de subverwerker ermee in dat de betrokkene een vordering kan instellen tegen de subverwerker, met betrekking tot diens eigen verwerkingsactiviteiten overeenkomstig deze bepalingen, alsof deze de gegevensexporteur of de gegevensimporteur was, tenzij een rechtsopvolger contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur of de gegevensimporteur heeft overgenomen, in welk geval de betrokkene zijn rechten tegenover die rechtsopvolger kan doen gelden. De aansprakelijkheid van de subverwerker blijft beperkt tot de verwerkingsactiviteiten die deze zelf heeft uitgevoerd overeenkomstig deze bepalingen. |

***Bepaling 7***

**Bemiddeling en rechtsmacht**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | De gegevensimporteur stemt ermee in dat, indien de betrokkene tegen hem rechten ten behoeve van derden en/of een vordering tot schadevergoeding krachtens de bepalingen inroept, hij de beslissing van de betrokkene aanvaardt:

|  |  |
| --- | --- |
| a) |  om het geschil te onderwerpen aan bemiddeling door een onafhankelijke persoon of, in voorkomend geval, door de toezichthoudende autoriteit; |

|  |  |
| --- | --- |
| b) |  om het geschil voor te leggen aan een rechterlijke instantie in de lidstaat waar de gegevensexporteur is gevestigd. |

 |

|  |  |
| --- | --- |
| 2. |  De partijen komen overeen dat de door de betrokkene gemaakte keuze geen afbreuk doet aan diens materiële of formele rechten om op grond van andere bepalingen van nationaal of internationaal recht verhaal te zoeken. |

***Bepaling 8***

**Samenwerking met de toezichthoudende autoriteiten**

|  |  |
| --- | --- |
| 1. |  De gegevensexporteur stemt ermee in een afschrift van dit contract bij de toezichthoudende autoriteit neer te leggen, indien deze daarom verzoekt of indien dit krachtens het toepasselijke recht inzake gegevensbescherming vereist is. |

|  |  |
| --- | --- |
| 2. |  De partijen komen overeen dat de toezichthoudende autoriteit bevoegd is bij de gegevensimporteur en eventuele subverwerkers een controle te verrichten die dezelfde reikwijdte heeft en aan dezelfde voorwaarden is onderworpen als die welke krachtens het toepasselijke recht inzake gegevensbescherming voor haar controle van de gegevensexporteur zouden gelden. |

|  |  |
| --- | --- |
| 3. |  Indien er wetgeving bestaat die op de gegevensimporteur of een subverwerker van toepassing is en die de uitvoering van controles als in lid 2 bedoeld op de gegevensimporteur of een subverwerker verbiedt, stelt de gegevensimporteur de gegevensexporteur daarvan onverwijld in kennis. In een dergelijk geval mag de gegevensexporteur de in bepaling 5, onder b), bedoelde maatregelen nemen. |

***Bepaling 9***

**Toepasselijk recht**

Op de bepalingen is het recht van de lidstaat van vestiging van de gegevensexporteur van toepassing, namelijk …

***Bepaling 10***

**Wijziging van het contract**

De partijen verbinden zich ertoe deze bepalingen niet te wijzigen. Dit vormt voor de partijen geen beletsel om indien nodig bepalingen toe te voegen betreffende met de transactie verband houdende vraagstukken, mits deze niet met deze modelcontractbepalingen in strijd zijn.

***Bepaling 11***

**Subverwerking**

|  |  |
| --- | --- |
| 1. |  De gegevensimporteur besteedt de verwerkingsactiviteiten die hij overeenkomstig deze bepalingen namens de gegevensexporteur uitvoert, niet uit zonder de voorafgaande schriftelijke toestemming van de gegevensexporteur. Indien de gegevensimporteur met toestemming van de gegevensexporteur zijn verplichtingen uit hoofde van deze bepalingen uitbesteedt, dient hij met de subverwerker een schriftelijk contract te sluiten waarbij aan de subverwerker dezelfde verplichtingen worden opgelegd als die waaraan de gegevensimporteur uit hoofde van deze bepalingen moet voldoen[(3)](https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32010D0087&from=NL#ntr3-L_2010039NL.01001001-E0003). Indien de subverwerker niet voldoet aan zijn verplichtingen inzake gegevensbescherming uit hoofde van dat schriftelijke contract, blijft de gegevensimporteur jegens de gegevensexporteur volledig aansprakelijk voor de uitvoering van de verplichtingen van de subverwerker uit hoofde van dat contract. |

|  |  |
| --- | --- |
| 2. |  In het tevoren tussen de gegevensimporteur en de subverwerker te sluiten schriftelijke contract dient tevens een derdenbeding te zijn opgenomen zoals vervat in bepaling 3, dat voorziet in gevallen waarin de betrokkene geen vordering tot schadevergoeding als bedoeld in bepaling 6, lid 1, kan instellen tegen de gegevensexporteur of de gegevensimporteur omdat deze feitelijk zijn verdwenen, hebben opgehouden rechtens te bestaan of insolvent zijn geworden, en er geen rechtsopvolger is die contractueel of rechtens alle wettelijke verplichtingen van de gegevensexporteur of de gegevensimporteur heeft overgenomen. Deze burgerlijke aansprakelijkheid van de subverwerker blijft beperkt tot de verwerkingsactiviteiten die deze zelf heeft uitgevoerd overeenkomstig deze bepalingen. |

|  |  |
| --- | --- |
| 3. |  Op de in lid 1 bedoelde bepalingen betreffende de gegevensbeschermingsaspecten van de subverwerking uit hoofde van het in lid 1 bedoelde contract is het recht van de lidstaat van vestiging van de gegevensexporteur van toepassing, namelijk … |

|  |  |
| --- | --- |
| 4. |  De gegevensexporteur houdt een lijst bij van subverwerkingscontracten die krachtens deze bepalingen zijn gesloten en door de gegevensimporteur overeenkomstig bepaling 5, onder j), zijn gemeld, en werkt deze ten minste eenmaal per jaar bij. Deze lijst wordt ter beschikking gesteld van de toezichthoudende autoriteit voor gegevensbescherming die op de gegevensexporteur toezicht houdt. |

***Bepaling 12***

**Verplichting na de beëindiging van de verwerking van persoonsgegevens**

|  |  |
| --- | --- |
| 1. |  De partijen komen overeen dat de gegevensimporteur en de subverwerker na het beëindigen van de verlening van de gegevensverwerkingsdiensten alle doorgegeven persoonsgegevens en kopieën daarvan aan de gegevensexporteur terugbezorgen of, indien de gegevensexporteur dat verkiest, alle persoonsgegevens vernietigen en aan de gegevensexporteur verklaren dat de vernietiging heeft plaatsgevonden, tenzij de op de gegevensimporteur toepasselijke wetgeving hem verbiedt alle of een gedeelte van de doorgegeven persoonsgegevens terug te bezorgen of te vernietigen. In dat geval garandeert de gegevensimporteur dat hij de vertrouwelijkheid van de doorgegeven persoonsgegevens zal respecteren en dat hij de doorgegeven gegevens niet verder actief zal verwerken. |

|  |  |
| --- | --- |
| 2. |  De gegevensimporteur en de subverwerker garanderen dat zij op verzoek van de gegevensexporteur en/of de toezichthoudende autoriteit hun verwerkingsvoorzieningen voor een controle van de in lid 1 bedoelde maatregelen beschikbaar zullen stellen. |

1. Europese Verordening nr. 2016/679 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 (AVG Algemene verordening gegevensbescherming). [↑](#footnote-ref-1)
2. Een “inbreuk in verband met persoonsgegevens” is een inbreuk op de beveiliging die resulteert in een accidentele of onwettige vernietiging, verlies, wijziging, niet-geautoriseerde vrijgave van of toegang tot persoonsgegevens. [↑](#footnote-ref-2)