MyExports

een must-have voor uw gemeente

MyExports

Verwerking persoonsgegevens (AVG)

Beveiliging persoonsgegevens

Versie 1.0 14 mei 2018

Versie 2.0 20 november 2019

Verantwoordelijke	
Naam	Hennie Jussen
Adres	Eilenbergstraat 233
Postcode en woonplaats	5011 EA Tilburg
Telefoonnummer	06-36427902
Algemeen emailadres	Hennie.jussen@myexports.nl

Verwerkers

Henk Koops, henk.koops@myexports.nl

Claudia Vansimpsen, claudia.vansimpsen@myexports.nl

Beveiliging

Organisatorische en technische maatregelen

- Logische toegangscontrole, gebruik makend van o.a. wachtwoorden
- Automatische logging van alle handelingen rond de persoonsgegevens
- Fysieke maatregelen voor toegangsbeveiliging
- Inbraakalarm
- Encryptie (versleuteling) van digitale bestanden met persoonsgegevens
- Organisatorische maatregelen voor toegangsbeveiliging
- Steekproefsgewijze controle op naleving beleid
- Beveiliging van netwerkverbindingen via Secure Socket Layer (SSL) technologie
- Een beveiligd intern netwerk
- Een inbraakwerende kluis voor het bewaren van persoonsgegevens
- Doelgebonden toegangsbeperkingen
- Controle op toegekende bevoegdheden

Doorgifte persoonsgegevens naar het buitenland

Niet van toepassing.

Wie heeft toegang tot persoonsgegevens?

Verantwoordelijke en verwerkers, op het geval van inbellen op het lokale netwerk van de klant.

Worden er persoonsgegevens verzameld middels profiling?

Nee.

Hoe worden betrokkenen geïnformeerd over de verwerking van gegevens die rechtstreeks bij hem/haar verkregen zijn?

Niet van toepassing.

Privacyverklaring website

Contactformulier

Onze website www.myexports.nl bevat een contactformulier. Als u het contactformulier op onze website invult of ons een e-mail stuurt, worden de gegevens die u ons toestuurt bewaard zolang als dat nodig is om uw e-mail volledig te beantwoorden en af te handelen.

LinkedIn

Op onze website zijn social media-buttons opgenomen. Hiermee verzamelen de beheerders van deze diensten uw persoonsgegevens. U bent zelf verantwoordelijk voor het klikken op deze buttons en het daarmee kenbaar maken van uw persoonsgegevens aan de beheerders van deze diensten. Dit gebeurt buiten onze invloedssfeer, wij zijn hier dan ook niet voor aansprakelijk.

Lees de privacyverklaring van LinkedIn om te lezen wat zij met de persoonsgegevens doen die zij van u verzamelen middels klikbuttons.

Websites van derden
Deze website is door middel van links verbonden met websites van derden. We kunnen niet garanderen dat deze derden op een betrouwbare of veilige manier met uw persoonsgegevens omgaan. Wij raden u aan de privacyverklaring van deze organisaties te lezen voordat u van deze websites gebruik maakt.

U heeft een klacht?

Heeft uw klacht betrekking op de verwerking van uw persoonsgegevens door ons, en komen wij er samen niet uit, dan kunt u zich altijd wenden tot de Autoriteit Persoonsgegevens. Postbus 93374 2509 AJ Den Haag, telefoon: 0900 – 200 12 01, e-mail: info@autoriteitpersoonsgegevens.nl, internet: www.autoriteitpersoonsgegevens.nl.
Aan de behandeling van uw klacht zijn voor u geen kosten verbonden.

Wijziging van deze verklaring

Wij behouden ons het recht voor om wijzigingen aan te brengen in deze verklaring. Wanneer u onze verklaring regelmatig raadpleegt, bent u van deze wijzigingen op de hoogte.

Tilburg, 14 mei 2018

Algemene
Verordening
Gegevensbescherming

Gegevensverwerking MyExports in beeld

Welke persoonsgegevens verwerkt MyExports, met welk doel?

Doel is om gegevens uit databases van verschillende leveranciers op een praktische wijze te ontsluiten en te rapporteren.

MyExports brengt informatie uit diverse gegevensbronnen samen en geeft de klant de mogelijkheid om relevante informatie te sorteren, combineren en rapporteren. Of het nou gaat om informatie over personen, bedrijven of van financiële aard.

MyExports is een dienstverleningsproduct dat gegevens uit allerlei bronnen controleert en veilig verspreidt naar gebruikers die daarvoor geautoriseerd zijn. Uiteraard wordt rekening gehouden met de eisen op het gebied van privacy en wetgeving. MyExports is bedoeld voor medewerkers van gemeentes en lokale overheden die bijvoorbeeld kwaliteitscontroles uitvoeren.

MyExports transformeert gegevens uit diverse bronnen naar een vast formaat of een database. Vanuit deze database kan de klant gegevens naar eigen inzicht selecteren, sorteren, ordenen, samenvoegen en vergelijken. Ook kan de klant eigen csv-bestanden toevoegen en deze combineren met de overige gegevens. Vervolgens start hij of zij bestaande rapporten of maakt hij of zij eigen rapporten in de gewenste lay-out en visualiseert deze aan de hand van heldere grafieken.

Alle gegevens kunnen door ons anoniem worden gemaakt door bsn, anr, naam, voorletters, achternaam en straat, woonplaats, postcode e.d. te vervangen door andere waarden. Alle Jansen worden bijv. (willekeurig) Pietersen. Voordeel is dat het leesbaar blijft, maar dat gezinsrelaties e.d. blijven bestaan. Ook het anonimiseren van data kan als apart product worden afgenomen.

Waar moeten deze gegevens vandaan komen en met wie worden ze gedeeld?

MyExports is een applicatie die lokaal bij de klant draait. Er is geen verkeer naar buiten vanuit de applicatie. MyExports leest gegevens vanuit diverse lokale bronnen (databases) in de organisatie en verzamelt deze in eenvoudig toegankelijke tabellen in een Oracle Database die ook lokaal op het systeem van de klant draait. Alle privacygevoelige gegevens die MyExports verwerkt staan dus in een speciale directory op een server lokaal bij de klant. Deze directory moet beveiligd zijn door de klant tegen onbevoegde toegang.

Verder staan de gegevens in een Oracle Database die ook beveiligd moet zijn door de klant tegen onbevoegde toegang.

Als verwerker bellen we bij u in via bijvoorbeeld Teamviewer om nieuwe rapporten te maken of storingen te verhelpen. Daarbij worden gegevens alleen via MyExports benaderd op het lokale systeem van de klant. Geen van deze gegevens wordt ooit overgenomen of gekopieerd naar andere systemen. Nieuwe rapporten en dergelijke kunnen wij dus ook alleen maken door gebruik te maken van MyExports op het lokale systeem van de klant, omdat wij zelf deze gegevens of bestanden niet ter beschikking hebben.

Onderstaande gegevens kunnen we mogelijk inzien op het lokale systeem van de klant.

- Objectgegevens (gestolen of verloren identiteitsbewijzen)
- Gegevens van overledenen of rechtspersonen
- Telefoonnummers, kentekens en postcodes; context
- Gegevens kadaster
- Direct identificeerbare gegevens
- Indirect identificeerbare gegevens

Nogmaals, geen van deze gegevens wordt ooit overgenomen of gekopieerd naar andere systemen. De toegang die wij hebben tot deze gegevens, komen vanuit een gerechtvaardigd belang om de gegevens te verwerken voor de klant. De gegevens zijn voor ons dus geen doel op zich, enkel de verwerking ervan is voor MyExports relevant. Deze verwerking ligt echter bij de klant.

Specifieke maatregelen

Voor applicaties waarin vertrouwelijke gegevens worden opgeslagen, is een goede beveiliging van groot belang. MyExports heeft daarom verschillende maatregelen getroffen die de betrouwbaarheid van de applicatie waarborgen.

Authenticatie

MyExports bestaat uit programmatuur die draait op servers op het interne netwerk. Deze programmatuur is standaard niet beschikbaar gemaakt voor gebruikers en wordt op deze manier afgeschermd. De regie over deze rechten is in handen van de beheerder(s) van uw organisatie. U kunt dus exact instellen welke rechten u aan een gebruiker toekent.

Authorisatie van en via de gegevensbeheerder

Alleen de MyExports_manager wordt door U aan een beperkt aantal gebruikers (gegevensbeheerders en raadplegers) ter beschikking gesteld. Via de MyExports_Manager kan de gegevensbeheerder, die bevoegd is om de gegevens van uw organisatie te beheren, de exportbestanden en rapportagebestanden samenstellen, inplannen en distribueren voor de gebruikers van uw organisatie. De verzending van de rapportages verloopt via het interne netwerk naar persoonlijke folders van de eindgebruikers. Zo wordt door uw gegevensbeheerder(s) expliciet geregeld dat eindgebruikers alleen over die data beschikken waartoe ze het recht hebben die in te zien. Raadplegers krijgen alleen de rapporten te zien die ter beschikking zijn gesteld door de gegevensbeheerders.

Uitgebreide logging

In MyExports wordt in de logging bijgehouden welke acties precies plaatsvinden. Welk rapport wordt aan wie verstrekt?

Van de batchverwerking en de interactief gestarte rapportages wordt volledig bijgehouden wie het start, voor wie het is bestemd, om welk rapport het gaat en op welke datum en tijd het wordt verstuurd.

Logging in 'exports'

In het tabblad 'exports' zijn drie rapportages te vinden die logging betreffende historie in MyExports weergeven. Het gaat hier om rapportages 368, 369 en 398: 'Logging betreffende historie aanmelden in MyExports' en 'Logging betreffende historie alle acties in MyExports' en 'Logging betreffende verstuurde rapportages'. Middels deze rapportages kan verantwoording AVG worden afgelegd.

368	Logging betreffende historie aanmelden in MyExports	Log	###Myexports_E	Logging	AVG
369	Logging betreffende historie alle acties in MyExports	Log	###Myexports_E	Logging	AVG
398	Logging betreffende verstuurde rapportages	Log	###Myexports_E	Logging	AVG

Rapport 'logging' (12) kan eventueel ook worden gebruikt als verantwoording.

12	Logging	Log	###Myexports_E	Logging	AVG

	A	B	C	D	E	F
1	LOGACT	LOGDATUM	LOGFILE	LOGMS	LOGMSGS	LOGMDW
2	E	2017-11-13 13:22:06	E:\Dropbox\Werkomgeving\MyExports_Basis\Exports\Rpt12_Koggenland_Logging_20171113132156.xlsx	Export 12	I	ontwikkelaar
3	E	2017-11-13 13:22:23	E:\Dropbox\Werkomgeving\MyExports_Basis\Exports\Rpt12_Koggenland_Logging_20171113132217.xlsx	Export 12	I	ontwikkelaar

Protocollering

Omdat een burger ook altijd zou kunnen vragen welke gegevens zijn verstrekt aan wie, zijn we bij MyExports bezig met protocollering. Ook protocollering gaan we toevoegen aan ons product, waarbij vastgelegd wordt over welke personen een bepaald rapport gaat (a-nummer, bsn). Dit is uniek ten opzichte van veel andere rapportagetools!

Netwerktoegang

MyExports draait op het eigen netwerk van de organisatie en kan daarom van de door de organisatie gebruikte netwerkbeveiliging en protocollen gebruik maken.

Databasetoegang

Om gegevens uit de brondatabase op te kunnen halen is toegang via een gebruiker en wachtwoord nodig. Om de toegang batchmatig in te kunnen stellen moeten deze inloggegevens worden opgeslagen. MyExports bewaart deze inloggegevens encrypted op een veilige plek.

Versiebeheer

Alle software componenten die MyExports gebruiken beschikken over een versienummer en worden ook dusdanig beheerd. Aanpassingen in de software kunnen hierdoor gecontroleerd plaatsvinden. Bovendien is de software status hierdoor bij de klant altijd direct duidelijk.

Gegevensverwerking Pepperflow Connector in beeld

Welke persoonsgegevens verwerkt met de Pepperflow Connector, met welk doel?

Doel is om uit databases van verschillende leveranciers op een praktische wijze financiële gegevens te ontsluiten en te transformeren naar de Pepperflow importstructuur.

De Pepperflow Connector brengt financiële informatie uit diverse gegevensbronnen samen en transformeert deze naar het door Pepperflow gewenste importformaat.

Waar moeten deze gegevens vandaan komen en met wie worden ze gedeeld?

Pepperflow Connector is een applicatie die lokaal bij de klant draait. Er is alleen verkeer naar buiten vanuit de applicatie. Pepperflow Connector leest gegevens vanuit diverse lokale bronnen (databases) in de organisatie en verzamelt deze in eenvoudig toegankelijke tabellen in een Oracle of SqlServer Database die ook lokaal op het systeem van de klant draait. Alle privacygevoelige gegevens die Pepperflow Connector verwerkt staan dus in een speciale directory op een server lokaal bij de klant. Deze directory moet beveiligd zijn door de klant tegen onbevoegde toegang.

Verder staan de gegevens in een Oracle of SqlServer Database die ook beveiligd moet zijn door de klant tegen onbevoegde toegang.

Als verwerker bellen we bij u in via bijvoorbeeld Teamviewer om nieuwe versies te installeren of storingen te verhelpen. Daarbij worden gegevens alleen via Pepperflow Connector benaderd op het lokale systeem van de klant. Geen van deze gegevens wordt ooit overgenomen of gekopieerd naar andere systemen. Nieuwe scripts en dergelijke kunnen wij dus ook alleen maken door gebruik te maken van Pepperflow Connector op het lokale systeem van de klant, omdat wij zelf deze gegevens of bestanden niet ter beschikking hebben.

Onderstaande gegevens kunnen we mogelijk inzien op het lokale systeem van de klant.

- Objectgegevens
- Gegevens van personen en bedrijven
- Telefoonnummers, kentekens en postcodes; context
- Direct identificeerbare gegevens
- Indirect identificeerbare gegevens

Nogmaals, geen van deze gegevens wordt ooit overgenomen of gekopieerd naar andere systemen. De toegang die wij hebben tot dee gegevens, komen vanuit een gerechtvaardigd belang om de gegevens te verwerken voor de klant. De gegevens zijn voor ons dus geen doel op zich, enkel de verwerking ervan is voor Pepperflow Connector relevant. Deze verwerking ligt echter bij de klant.

Bij de huidige aanlevering van gegevens aan Pepperflow geldt daarbij nog extra dat deze eigenlijk geen privacygevoelige info bevat als bsn, of bankrekening of naw van een persoon.

Specifieke maatregelen Pepperflow Connector

Voor applicaties waarin vertrouwelijke gegevens worden opgeslagen, is een goede beveiliging van groot belang. Pepperflow Connector heeft daarom verschillende maatregelen getroffen die de betrouwbaarheid van de applicatie waarborgen.

Authenticatie

Pepperflow Connector bestaat uit programmatuur die draait op servers op het interne netwerk. Deze programmatuur is standaard niet beschikbaar voor gebruikers en wordt op deze manier afgeschermd. De programmatuur draait alleen in batch geregisseerd via de windows schedular.

Uitgebreide logging

In Pepperflow Connector wordt in de logging bijgehouden welke acties precies plaatsvinden. Welke bestanden worden precies aangemaakt en hoeveel records worden er naar Pepperflow verstuurd? Verder worden alle verstuurde bestanden en mutaties op het systeem van de klant gearchiveerd.

Netwerktoegang

Pepperflow Connector draait op het eigen netwerk van de organisatie en kan daarom van de door de organisatie gebruikte netwerkbeveiliging en protocollen gebruik maken.

Databasetoegang

Om gegevens uit de brondatabase op te kunnen halen is toegang via een gebruiker en wachtwoord nodig. Om de toegang batchmatig in te kunnen stellen moeten deze inloggegevens worden opgeslagen. Pepperflow Connector bewaart deze inloggegevens encrypted op een veilige plek.

Versiebeheer

Alle software componenten die Pepperflow Connector gebruiken beschikken over een versienummer en worden ook dusdanig beheerd. Aanpassingen in de software kunnen hierdoor gecontroleerd plaatsvinden. Bovendien is de software status hierdoor bij de klant altijd direct duidelijk.

Gegevensverwerking webbrowsers in beeld

Welke persoonsgegevens verwerken de webbrowsers (statistiek, archieven, raadplegen en monitor) van MyExports, met welk doel?

Doel is (afhankelijk van het specifieke product) om gegevens uit databases te tonen en eventueel te combineren, te archiveren, te bekijken en te beheren.

MyExports_Statistiek is een tooling om een dashboardfunctie en het tonen van managementinfo te combineren.
MyExports_Archief vergemakkelijkt het archiveren van gegevens en het opvragen, combineren en raadplegen van specifieke informatie uit verschillende databases.
MyExports_Raadplegen is een tooling voor het tonen van gegevens uit een applicatie of van gegevens van een rapportage uit een applicatie.
MyExports_Monitor kan een beheertool als Nagios van de noodzakelijk informatie voorzien, waardoor de technische beheerders bij mogelijk aankomende problemen preventief met de desbetreffende gebruikers en/of applicatiebeheerder contact op kan nemen.

In bovenstaande webbrowser-producten kan het gaan om informatie over personen, bedrijven of van financiële aard. We spreken over browserapplicaties, waarmee je via een url de benodigde informatie kunt raadplegen.

Deze MyExports webbrowsers zijn allen dienstverleningsproducten die gegevens uit allerlei bronnen controleren en veilig verspreiden naar gebruikers die daarvoor geautoriseerd zijn. Uiteraard wordt rekening gehouden met de eisen op het gebied van privacy en wetgeving. De producten zijn bedoeld voor medewerkers van gemeentes en lokale overheden die bijvoorbeeld kwaliteitscontroles uitvoeren.

Alle gegevens kunnen door ons anoniem worden gemaakt door bsn, anr, naam, voorletters, achternaam en straat, woonplaats, postcode e.d. te vervangen door andere waarden. Alle Jansen worden bijv. (willekeurig) Pietersen. Voordeel is dat het leesbaar blijft, maar dat gezinsrelaties e.d. blijven bestaan.

Waar moeten deze gegevens vandaan komen en met wie worden ze gedeeld?

Er is geen verkeer naar buiten vanuit de browsers. MyExports leest gegevens vanuit diverse lokale bronnen (databases) in de organisatie en verzamelt deze in eenvoudig toegankelijke tabellen in een Oracle Database die ook lokaal op het systeem van de klant draait. Alle privacygevoelige gegevens die MyExports verwerkt staan dus in een speciale directory op een server lokaal bij de klant. Deze directory moet beveiligd zijn door de klant tegen onbevoegde toegang.

Verder staan de gegevens in een Oracle Database die ook beveiligd moet zijn door de klant tegen onbevoegde toegang.

Als verwerker bellen we bij u in via bijvoorbeeld Teamviewer. Daarbij worden gegevens alleen via MyExports benaderd op het lokale systeem van de klant. Geen van deze gegevens wordt ooit overgenomen of gekopieerd naar andere systemen. Nieuwe rapporten en dergelijke kunnen wij dus ook alleen maken door gebruik te maken van MyExports op het lokale systeem van de klant, omdat wij zelf deze gegevens of bestanden niet ter beschikking hebben.

Onderstaande gegevens kunnen we mogelijk inzien op het lokale systeem van de klant.

- Objectgegevens (gestolen of verloren identiteitsbewijzen)
- Gegevens van overledenen of rechtspersonen
- Telefoonnummers, kentekens en postcodes; context
- Gegevens kadaster
- Direct identificeerbare gegevens
- Indirect identificeerbare gegevens

Nogmaals, geen van deze gegevens wordt ooit overgenomen of gekopieerd naar andere systemen. De toegang die wij hebben tot deze gegevens, komen vanuit een gerechtvaardigd belang om de gegevens te verwerken voor de klant. De gegevens zijn voor ons dus geen doel op zich, enkel de verwerking ervan is voor MyExports relevant. Deze verwerking ligt echter bij de klant.

Specifieke maatregelen webbrowsers

Voor applicaties waarin vertrouwelijke gegevens worden opgeslagen, is een goede beveiliging van groot belang. MyExports heeft daarom verschillende maatregelen getroffen die de betrouwbaarheid van de applicatie waarborgen.

Authenticatie

De webbrowsers van MyExports draaien op geautoriseerde servers op het interne netwerk. Deze programmatuur is standaard niet beschikbaar gemaakt voor gebruikers en wordt op deze manier afgeschermd. De regie over deze rechten is in handen van de beheerder(s) van uw organisatie. U kunt dus exact instellen welke rechten u aan een gebruiker toekent.

Authorisatie van en via de gegevensbeheerder

De verschillende webbrowsers worden door ons aan een beperkt aantal gebruikers (gegevensbeheerders) ter beschikking gesteld. De gegevensbeheerders, die bevoegd zijn om de gegevens van uw organisatie te beheren, mogen de gebruikers van de specifieke webbrowser binnen uw organisatie bepalen. Zo wordt door uw gegevensbeheerder(s) expliciet geregeld dat eindgebruikers alleen over die data beschikken waartoe ze het recht hebben die in te zien.

Uitgebreide logging

In de webbrowsers van MyExports wordt in de logging bijgehouden welke acties precies plaatsvinden.

Netwerktoegang

MyExports draait op het eigen netwerk van de organisatie en kan daarom van de door de organisatie gebruikte netwerkbeveiliging en protocollen gebruik maken.

Databasetoegang

Om gegevens uit de brondatabase op te kunnen halen is toegang via een gebruiker en wachtwoord nodig.

Versiebeheer

Alle softwarecomponenten die MyExports gebruiken beschikken over een versienummer en worden ook dusdanig beheerd. Aanpassingen in de software kunnen hierdoor gecontroleerd plaatsvinden. Bovendien is de softwarestatus hierdoor bij de klant altijd direct duidelijk.

MyExports

Verwerking persoonsgegevens (AVG)

Voorbeeld van verwerkersovereenkomst (bijlage bij leveringsvoorwaarden)

Jussen Ict vof
Eilenbergstraat 233
5011 EA Tilburg
013-4552801
06-36427902
www.jussenict.nl
jussen@jussenict.nl

Inleiding

Indien Opdrachtnemer bij de uitvoering van de Overeenkomst ten behoeve van Opdrachtgever Persoonsgegevens verwerkt, zijn in aanvulling op de Algemene Voorwaarden de onderstaande voorwaarden van toepassing. De klant stelt met de Opdrachtnemer een Verwerkingsovereenkomst op, zoals bedoeld in artikel 14 lid 2[1] van de Wet bescherming persoonsgegevens (hierna: Wbp) en, vanaf 25 mei 2018, als bedoeld in artikel 28 lid 3 en 4[2], van de Algemene Verordening Gegevensbescherming (hierna: AVG), tussen de Opdrachtgever en de Opdrachtnemer.

In deze bijlage trachten wij aan te geven hoe wij aan de voorwaarden voldoen betreffende onze dienstverlening met MyExports. Waar in deze Verwerkingsovereenkomst termen worden gebruikt die overeenstemmen met definities uit artikel 4[3] van de AVG, wordt aan deze termen de betekenis van de definities uit de AVG toegekend.

Artikel 1. Algemeen

1. De begrippen die in deze Bijlage worden gedefinieerd in de Algemene Verordening Gegevensbescherming (hierna: “AVG”) hebben de betekenis die daaraan in de AVG is toegekend.

2. Bij de verwerking van Persoonsgegevens kan Opdrachtgever worden aangemerkt als Opdrachtgever, of indien Opdrachtgever de Persoonsgegevens ten behoeve van een derde partij verwerkt als Opdrachtnemer. Opdrachtnemer vervult (afhankelijk van de hoedanigheid waarin de Opdrachtgever Persoonsgegevens verwerkt) de rol van Opdrachtnemer of subOpdrachtnemer.

2.1 (Verwerkings-)verantwoordelijke: 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.

2.2 Opdrachtnemer: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Opdrachtgever persoonsgegevens verwerkt. Degene die ten behoeve van de Opdrachtgever persoonsgegevens verwerkt, in opdracht van de Opdrachtnemer, is een sub-Opdrachtnemer.

3. Toezichthouder: de Autoriteit Persoonsgegevens (AP) is het zelfstandig bestuursorgaan dat in Nederland bij wet als toezichthouder is aangesteld voor het toezicht op het verwerken van persoonsgegevens.

Artikel 2. Doeleinden van de verwerking

1. Opdrachtnemer verbindt zich ertoe om onder de voorwaarden uit de Overeenkomst in opdracht van Opdrachtgever Persoonsgegevens te verwerken. De verwerking zal uitsluitend plaatsvinden in het kader van het uitvoeren van de Overeenkomst , plus die doeleinden die daarmee redelijkerwijs samenhangen of die met nadere instemming worden bepaald.

---

1 [1] Artikel 14, lid 2 Wbp*: De uitvoering van verwerkingen door een bewerker wordt geregeld in een overeenkomst of krachtens een andere rechtshandeling waardoor een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.*

[2] Artikel 28, lid 3 en 4 (AVG): zie http://www.privacy-regulation.eu/nl/artikel-28-Opdrachtnemer-EU-AVG.htm.

[3] Zie voor een volledig overzicht van de definities: http://www.privacy-regulation.eu/nl/artikel-4-definities-EU-AVG.htm.

2. Opdrachtnemer zal de persoonsgegevens niet voor enig ander doel verwerken dan zoals door Opdrachtgever is vastgesteld.

2.2 De Opdrachtnemer verbindt zich om in het kader van die werkzaamheden, omschreven in addendum 1 onderaan deze bijlage, de door of via de Opdrachtgever ter beschikking gestelde persoonsgegevens zorgvuldig te verwerken.

3. Opdrachtnemer heeft geen zeggenschap over het doel en de middelen voor de verwerking van Persoonsgegevens. Opdrachtnemer neemt geen beslissingen over de ontvangst en het gebruik van de Persoonsgegevens, de verstrekking aan derden en de duur van de opslag van Persoonsgegevens.

Artikel 3. Verplichtingen Opdrachtnemer

1. Ten aanzien van de in artikel 2 genoemde verwerkingen zal Opdrachtnemer zorg dragen voor de naleving van de voorwaarden die, op grond van de AVG, worden gesteld aan het verwerken van Persoonsgegevens.

2. Opdrachtnemer zal Persoonsgegevens en andere gegevens verwerken die door of namens de Opdrachtgever aan Opdrachtnemer zullen worden aangeleverd.

3. Opdrachtnemer zal Opdrachtgever, op diens verzoek daartoe en binnen een redelijke termijn, informeren over de door haar genomen maatregelen aangaande haar verplichtingen onder deze Bijlage.

4. De verplichtingen van Opdrachtnemer die uit deze Bijlage voortvloeien, gelden ook voor degenen die Persoonsgegevens verwerken onder het gezag van Opdrachtnemer.

5. Opdrachtnemer zal Opdrachtgever in kennis stellen indien naar zijn mening een instructie van Opdrachtgever in strijd is met relevante privacywet- en regelgeving. De instructie als zodanig wordt dan niet door de Opdrachtnemer uitgevoerd. Opdrachtgever en Opdrachtnemer gaan in gesprek om de instructie, indien mogelijk, te herformuleren.

6. Opdrachtnemer zal Opdrachtgever de noodzakelijke medewerking verlenen wanneer er in het kader van de verwerking een gegevensbeschermingseffectbeoordeling, of voorafgaande raadpleging van de toezichthouder, noodzakelijk mocht zijn.

7. Indien de Opdrachtnemer op grond van een wettelijke verplichting gegevens dient te verstrekken, zal de Opdrachtnemer de grondslag van het verzoek en de identiteit van de verzoeker verifiëren en zal de Opdrachtnemer de Opdrachtgever ter zake informeren. Tenzij wettelijke bepalingen dit verbieden.

Artikel 4. Doorgifte van persoonsgegevens

1. Opdrachtnemer mag de persoonsgegevens verwerken in landen binnen en buiten de Europese Unie, met inachtneming van de relevante wet- en regelgeving.

2. Opdrachtnemer zal Opdrachtgever, op diens verzoek daartoe, melden om welk land of landen het gaat.

Artikel 5. Verdeling van verantwoordelijkheid

1. Partijen zullen zorg dragen voor de naleving van toepasselijke privacywet- en regelgeving.

2. De toegestane verwerkingen zullen door Opdrachtnemer worden uitgevoerd binnen een (semi-) geautomatiseerde omgeving.

3. Opdrachtnemer is louter verantwoordelijk voor de verwerking van de Persoonsgegevens onder deze Bijlage, overeenkomstig de instructies van Opdrachtgever en onder de uitdrukkelijke (eind)verantwoordelijkheid van Opdrachtgever. Voor alle overige verwerkingen van Persoonsgegevens, waaronder in ieder geval begrepen maar niet beperkt tot de verzameling van de Persoonsgegevens door Opdrachtgever, verwerkingen voor doeleinden die niet door Opdrachtgever aan Opdrachtnemer zijn gemeld, verwerkingen door derden en/of voor andere doeleinden, is

Opdrachtnemer niet verantwoordelijk. De verantwoordelijkheid voor deze verwerkingen rust uitsluitend bij Opdrachtgever.

4. Opdrachtgever staat ervoor in dat de inhoud, het gebruik en de opdracht tot verwerkingen van Persoonsgegevens, zoals bedoeld in deze Bijlage, niet onrechtmatig is en geen inbreuk maakt op enig recht van derden.

Artikel 6. Inschakelen van derden of onderaannemers

1. Opdrachtgever verleent Opdrachtnemer hierbij toestemming om bij de verwerking derden (subOpdrachtnemers) in te schakelen.

2. Op verzoek van Opdrachtgever zal Opdrachtnemer Opdrachtgever zo spoedig mogelijk informeren over de door haar ingeschakelde subOpdrachtnemers. Opdrachtgever heeft het recht om bezwaar te maken tegen het inschakelen van een subOpdrachtnemer. Dit bezwaar dient schriftelijk, binnen twee weken en door argumenten ondersteund, te worden ingediend.

3. Opdrachtnemer zorgt er onvoorwaardelijk voor dat deze derden schriftelijk dezelfde plichten op zich nemen als tussen Opdrachtgever en Opdrachtnemer zijn overeengekomen. Opdrachtnemer staat in voor een correcte naleving van deze plichten door deze derden.

4. De Opdrachtnemer houdt een actueel register bij van de door hem ingeschakelde derden en onderaannemers waarin de identiteit, vestigingsplaats en een beschrijving van de werkzaamheden van de derden of onderaannemers zijn opgenomen, alsmede eventuele door de Opdrachtgever gestelde aanvullende voorwaarden. Dit register zal als Addendum 5 aan deze bijlage worden toegevoegd en zal door de Opdrachtnemer actueel worden gehouden.

Artikel 7. Beveiliging

1. Opdrachtnemer zal zich inspannen passende technische en organisatorische maatregelen te nemen met betrekking tot de te verrichten verwerkingen van Persoonsgegevens, tegen verlies of tegen enige vorm van onrechtmatige verwerking (zoals onbevoegde kennisname, aantasting, wijziging of verstrekking van de persoonsgegevens). Zie addendum 2 van deze bijlage.

2. Opdrachtnemer staat er niet voor in dat de beveiliging onder alle omstandigheden doeltreffend is. Opdrachtnemer zal zich inspannen om de beveiliging te laten voldoen aan een niveau dat, gelet op de stand van de techniek, de gevoeligheid van de Persoonsgegevens en de aan het treffen van de beveiliging verbonden kosten, niet onredelijk is, overeenkomstig met artikel 13 van de Wbp en artikel 32 van de AVG en omschreven in addendum 2 van deze bijlage[4].

3. Opdrachtgever stelt enkel Persoonsgegevens ter verwerking aan Opdrachtnemer ter beschikking, indien Opdrachtgever zich ervan heeft verzekerd dat de vereiste beveiligingsmaatregelen zijn getroffen. Opdrachtgever is verantwoordelijk voor de naleving van de door Partijen afgesproken maatregelen.

---

[4] Artikel 13, Wbp: *De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.*

Artikel 32, AVG: http://www.privacy-regulation.eu/nl/artikel-32-beveiliging-van-de-verwerking-EU-AVG.htm

Artikel 8. Meldplicht

1. In het geval van een beveiligingslek en/of een datalek (waaronder wordt verstaan: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidde tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens) zal Opdrachtnemer, zich naar beste kunnen inspannen om Opdrachtgever daarover zo snel mogelijk te informeren naar aanleiding waarvan Opdrachtgever beoordeelt of zij de toezichthoudende autoriteiten en/of betrokkenen zal informeren of niet. Opdrachtnemer spant zich naar beste kunnen in om de verstrekte informatie volledig, correct en accuraat te maken.

2. Indien de wet- en/of regelgeving dit vereist zal Opdrachtnemer meewerken aan het op de kortst mogelijke termijn informeren van de relevante autoriteiten en eventueel betrokkenen. Opdrachtgever is verantwoordelijk voor het melden naar de relevante autoriteiten.

3. De meldplicht behelst in ieder geval het melden van het feit dat er een lek is geweest. Daarbij verschaft de Opdrachtnemer in ieder geval de informatie aan de Opdrachtgever zoals omschreven in addendum 3.

Artikel 9 Beveiligingsmaatregelen en controle

1. De Opdrachtnemer neemt alle passende technische en organisatorische maatregelen om de persoonsgegevens welke worden verwerkt ten dienste van de Opdrachtgever te beveiligen en beveiligd te houden tegen verlies of tegen enige vorm van onrechtmatige verwerking. De wijze van beveiliging wordt nader omschreven in addendum 4.

2. De Opdrachtgever is te allen tijde gerechtigd de verwerking van persoonsgegevens te (doen) controleren. De Opdrachtnemer is verplicht de Opdrachtgever, de Autoriteit Persoonsgegevens, of, de onder geheimhouding, controlerende instantie in opdracht van de Opdrachtgever toe te laten en verplicht medewerking te verlenen zodat de controle daadwerkelijk uitgevoerd kan worden.

3. De Opdrachtgever zal de controle slechts (laten) uitvoeren na een voorafgaande schriftelijke melding aan de Opdrachtnemer.

4. De Opdrachtnemer staat er voor in, de door de Opdrachtgever of ingeschakelde derde, aangegeven aanbevelingen ter verbetering binnen de daartoe door de Opdrachtgever te bepalen redelijke termijn uit te voeren.

5. Naast controles door de Opdrachtgever of controlerende instantie in opdracht van de Opdrachtgever, kunnen beide partijen ook overeenkomen gebruik te maken van een Third Party Memorandum (TPM) opgesteld door een onafhankelijke externe deskundige.

6. De redelijke kosten van de controle worden gedragen door de partij die de kosten maakt.

Artikel 10. Afhandeling verzoeken van betrokkenen

1. In het geval dat een betrokkene een verzoek over zijn persoonsgegevens richt aan Opdrachtgever, en blijkt dat de Opdrachtgever hulp benodigd heeft van Opdrachtnemer voor de uitvoering van het verzoek van de betrokkene, zal Opdrachtnemer hieraan meewerken en kan Opdrachtnemer hiervoor onverwijld kosten in rekening brengen. Opdrachtgever zal het verzoek vervolgens verder zelfstandig afhandelen.

Artikel 11. Geheimhouding en vertrouwelijkheid

1. Persoonsgegevens blijven binnen het domein van de Opdrachtgever, met uitzondering van niet-herleidbare, geanonimiseerde gegevens betreffende een (niet-natuurlijk) persoon.

2. Op alle Persoonsgegevens die direct of indirect te herleiden zijn naar een persoon of niet-natuurlijke persoon die Opdrachtnemer van Opdrachtgever ontvangt en/of zelf verzamelt in het kader

van deze Bijlage, rust een geheimhoudingsplicht jegens derden. Opdrachtnemer zal deze informatie niet voor een ander doel gebruiken dan waarvoor hij deze heeft verkregen en zal deze informatie op een veilige manier bewaren, wat betekent dat de gegevens niet toegankelijk zijn zonder een gecontroleerde toegang, beschikbaar gesteld door de Opdrachtnemer.

3. Deze geheimhoudingsplicht is niet van toepassing:
-Voor zover Opdrachtgever uitdrukkelijke toestemming heeft gegeven om de informatie aan derden te verschaffen; of
-Indien het verstrekken van de informatie aan derden logischerwijs noodzakelijk is voor de uitvoering van de Hoofdovereenkomst of deze Bijlage; en
-Indien er een wettelijke verplichting bestaat om de informatie aan een derde te verstrekken.

Artikel 12. Audit

1. Opdrachtgever heeft het recht om audits uit te laten voeren door een onafhankelijke ICT-deskundige die aan geheimhouding is gebonden ter controle van naleving van alle punten uit deze Bijlage.

2. Deze audit vindt uitsluitend plaats nadat Opdrachtgever de bij Opdrachtnemer aanwezige soortgelijke auditrapportages heeft opgevraagd, beoordeeld en redelijke argumenten aanbrengt die een door Opdrachtgever geïnitieerde audit alsnog rechtvaardigen. Een dergelijke audit wordt gerechtvaardigd wanneer de bij Opdrachtnemer aanwezige soortgelijke auditrapportages geen of onvoldoende uitsluitsel geven over het naleven van deze Bijlage door Opdrachtnemer.

3. Opdrachtnemer zal aan de audit meewerken en alle voor de audit redelijkerwijs relevante informatie, inclusief ondersteunende gegevens zoals systeemlogs (behoudens privacygevoelige gegevens van derden), en medewerkers zo tijdig mogelijk en binnen een redelijke termijn, waarbij een termijn van maximaal twee weken redelijk is tenzij een spoedeisend belang zich hiertegen verzet, ter beschikking stellen.

4. De bevindingen naar aanleiding van de uitgevoerde audit zullen door Partijen in onderling overleg worden beoordeeld en, naar aanleiding daarvan, al dan niet worden doorgevoerd door één van de Partijen of door beide Partijen gezamenlijk.

5. De redelijke kosten voor de audit worden door de Opdrachtgever gedragen, met dien verstande dat de kosten voor de in te huren ICT-deskundige altijd door Opdrachtgever zullen worden gedragen.

Artikel 13. Duur en opzegging

1. De Bijlage is aangegaan voor de duur zoals bepaald in de Overeenkomst tussen Partijen en bij gebreke daarvan in ieder geval voor de duur van de samenwerking.

2. De Bijlage kan tussentijds niet worden opgezegd.

3. Partijen mogen deze Bijlage alleen wijzigen met wederzijdse instemming.

4. Indien een partij tekort schiet in de nakoming van een overeengekomen verplichting, kan de andere partij haar in gebreke stellen waarbij de nalatige partij alsnog een redelijke termijn voor de nakoming wordt gegund. Blijft nakoming ook dan uit dan is de nalatige partij in verzuim. Ingebrekestelling is niet nodig wanneer voor de nakoming een fatale termijn geldt, nakoming blijvend onmogelijk is of indien uit een mededeling dan wel de houding van de andere partij moet worden afgeleid dat deze in de nakoming van haar verplichting zal tekortschieten.

5. Opdrachtgever is gerechtigd deze Verwerkingsovereenkomst en de hoofdovereenkomst per direct te ontbinden indien de Opdrachtnemer te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van de ontwikkelingen in de wet en/of de rechtspraak aan de verwerking van de persoonsgegevens worden gesteld.

Artikel 14. Toepasselijk recht

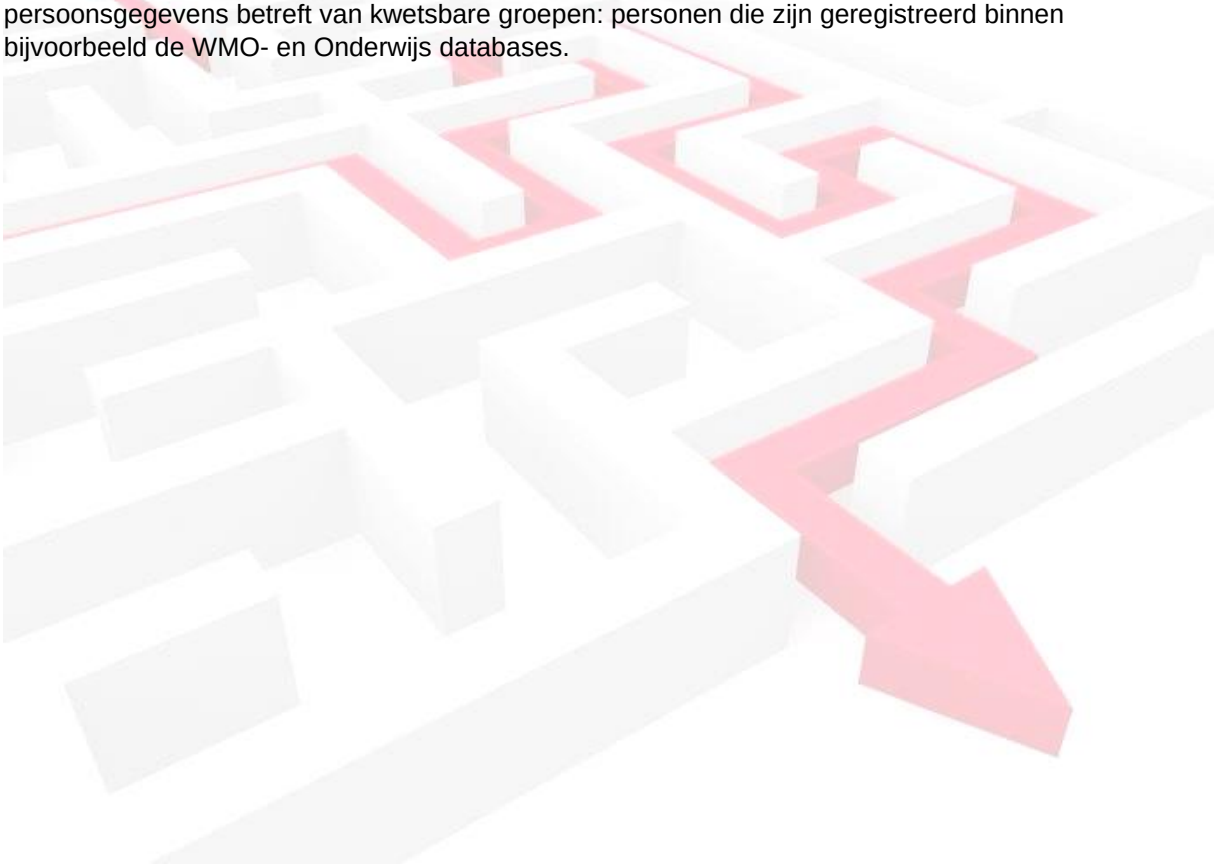
1. Op deze Verwerkingsovereenkomst en op alle geschillen die daaruit mogen voortvloeien of daarmee mogen samenhangen, is het Nederlands recht van toepassing.

Addendum 1: omschrijving werkzaamheden ter uitwerking van artikel 2.2

De werkzaamheden van de Opdrachtnemer (de verleende diensten en de bijbehorende verwerking): Een overzicht hiervan is te vinden in de leveringsvoorwaarden, op www.myexports.nl.

Werkzaamheden die plaatsvinden na installatie en ontsluiten databronnen:
Helpdesk bestaande uit activiteiten zoals inbellen via Teamviewer in geval er problemen zijn met de My Exports-omgeving. Daarnaast wordt ondersteuning geboden bij (problemen met) rapportages, zelfgebouwde of standaard ter beschikking gesteld binnen My-Exports. Het is hierbij reëel te veronderstellen dat Opdrachtnemer tijdens inbellen zicht krijgt op persoonsgegevens die zich binnen de My Exports-database bevinden. Deze worden echter nooit overgenomen of ergens opgeslagen.

Categorieën personen en soorten persoonsgegevens:
De persoonsgegevens die het betreft, zijn die van burgers van klantgemeenten en mogelijk ook van burgers woonachtig in andere gemeenten, afkomstig uit diverse databronnen. Het BSN zal in sommige gevallen daarvan een onderdeel zijn. Daarnaast is het ook mogelijk dat het persoonsgegevens betreft van kwetsbare groepen: personen die zijn geregistreerd binnen bijvoorbeeld de WMO- en Onderwijs databases.



Addendum 2: Beschrijving beveiliging ter uitwerking van artikel 7.1 en 7.2

Overzicht getroffen beveiligingsmaatregelen door Verwerker

Verwerker heeft in ieder geval de volgende maatregelen genomen:

- ☐ Logische toegangscontrole, gebruik makend van:
  - ☐ wachtwoorden
  - ☐ persoonsgebonden toegangspasjes
  - ☐ biometrische verificatie
- ☐ Automatische logging van alle handelingen rond de persoonsgegevens
- ☐ Fysieke maatregelen voor toegangsbeveiliging
- ☐ Inbraakalarm
- ☐ Encryptie (versleuteling) van digitale bestanden met persoonsgegevens
- ☐ Organisatorische maatregelen voor toegangsbeveiliging
- ☐ Steekproefsgewijze controle op naleving beleid
- ☐ Beveiliging van netwerkverbindingen via Secure Socket Layer (SSL) technologie
- ☐ Een beveiligd intern netwerk
- ☐ Een inbraakwerende kluis voor het bewaren van persoonsgegevens
- ☐ Doelgebonden toegangsbeperkingen
- ☐ Controle op toegekende bevoegdheden

1. **Normenstelsel:** De informatiebeveiliging vindt plaats volgens een algemeen erkende overheidsnorm: de BIG.
2. **De toereikendheid van de informatiebeveiliging blijkt uit:** Eigen controles en eigen mededelingen.
3. **Uit de certificering of periodieke externe controles of uit de audits of uit de eigen controles blijkt of kan afgeleid worden dat de beveiliging voldoet aan of gelijkwaardig is met de toelichting (addendum 4) en de daarin omschreven elementen.**

Addendum 3: Inlichtingen om incidenten te beoordelen ter uitwerking van artikel 8.3

De Opdrachtnemer zal alle inlichtingen verschaffen die de Opdrachtgever noodzakelijk acht om het incident te kunnen beoordelen. Daarbij verschaft de Opdrachtnemer in ieder geval de volgende informatie aan de Opdrachtgever:

- wat de (vermeende) oorzaak is van de inbreuk;
- wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- wat de (voorgestelde) oplossing is;
- contactgegevens voor de opvolging van de melding;
- aantal personen waarvan gegevens betrokken zijn bij de inbreuk (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens betrokken zijn bij de inbreuk);
- een omschrijving van de groep personen van wie gegevens betrokken zijn bij de inbreuk;
- het soort of de soorten persoonsgegevens die betrokken zijn bij de inbreuk;
- de datum waarop de inbreuk heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen de inbreuk heeft plaatsgevonden);
- de datum en het tijdstip waarop de inbreuk bekend is geworden bij de Opdrachtnemer of bij een door hem ingeschakelde derde of onderaannemer;
- of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden (geanonimiseerd);
- wat de reeds ondernomen maatregelen zijn om de inbreuk te beëindigen en om de gevolgen van de inbreuk te beperken.

Addendum 4: Maatregelen op basis van de BIG ten aanzien van een Opdrachtnemer, omschrijving bij artikel 9.1

Deze maatregelen zijn uit de BIG afkomstig en waar mogelijk specifiek gemaakt voor de Opdrachtnemer. Deze maatregelen gaan uit van het niveau van de BIG. Als de gegevens van de Opdrachtgever hoger geclassificeerd zijn, een hogere risico inschatting hebben (bijzondere persoonsgegevens) of extra maatregelen nodig hebben uit specifieke wetgeving, dan kan deze bijlage worden uitgebreid.

BIG Nummer	titel	Genomen maatregel door Opdrachtnemer
6.1.5.1	Geheimhoudingsovereenkomst	Medewerkers die te maken hebben met persoonsinformatie van de Opdrachtgever dienen een geheimhoudingsverklaring te ondertekenen. Hierbij wordt tevens vastgelegd dat na beëindiging van de functie, de betreffende persoon gehouden blijft aan die geheimhouding.
6.2.3.1	Beveiliging behandelen in overeenkomsten met een derde partij	Maatregelen uit de Verwerkingsovereenkomst zijn geïmplementeerd.
7.2.2.1	Labeling en verwerking van informatie	De Opdrachtnemer heeft maatregelen genomen zo dat niet geautoriseerden geen kennis kunnen nemen van persoonsgegevens.
8.1.1.2	Rollen en verantwoordelijkheden	Het personeel van de Opdrachtnemer of derden moeten kennis hebben van de verantwoordelijkheden ten aanzien van de bewerking van de persoonsgegevens voor de Opdrachtgever.
8.1.2.1	Screening	Voor personen is een recente Verklaring Omtrent het Gedrag (VOG) vereist met punten die door de Opdrachtgever zijn aangedragen. Tenzij dit centraal in het contract geregeld is.
8.3.3.1	Blokkering van toegangsrechten	Toegangsrechten van medewerkers van de Opdrachtnemer worden direct geblokkeerd als geen toegang voor de bewerking van de persoonsgegevens noodzakelijk is.
9.1.2.1	Fysieke toegangsbeveiliging	Toegang tot beveiligde zones of gebouwen waar persoonsgegevens van de Opdrachtgever zich bevinden is alleen mogelijk na autorisatie daartoe.
9.1.3.1	Beveiliging van kantoren, ruimten en faciliteiten	Papieren documenten en mobiele gegevensdragers die persoonsgegevens of andere vertrouwelijke gegevens van de Opdrachtgever bevatten worden beveiligd opgeslagen.

BIG Nummer	titel	Genomen maatregel door Opdrachtnemer
10.3.1.1	Capaciteitsbeheer	De ICT-voorzieningen voldoen aan het voor de dienst overeengekomen niveau van beschikbaarheid. Er worden voorzieningen geïmplementeerd om de beschikbaarheid van componenten te bewaken (bijvoorbeeld de controle op aanwezigheid van een component en metingen die het gebruik van een component vaststellen). Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen. Op basis van een risicoanalyse wordt bepaald wat de beschikbaarheidseis van een ICT-voorziening is en wat de impact bij uitval is. Afhankelijk daarvan worden maatregelen bepaald zoals automatisch werkende mechanismen om uitval van (fysieke) ICT-voorzieningen, waaronder verbindingen op te vangen.
10.6.1.2	Maatregelen voor netwerken	Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
10.6.1.3	Maatregelen voor netwerken	Bij transport van vertrouwelijke informatie over niet vertrouwde netwerken tussen de Opdrachtnemer en de Opdrachtgever, zoals over het internet, dient altijd geschikte encryptie te worden toegepast. Zie hiertoe 12.3.1.3.
10.8.2.2	Uitwisselingsovereenkomsten	Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten zijn beschreven, evenals procedures over melding van incidenten van de Opdrachtnemer naar de Opdrachtgever.
10.8.3.1	Fysieke media die worden getransporteerd	De Opdrachtnemer neemt maatregelen om vertrouwelijke informatie te beschermen, zoals: • Versleuteling. • Bescherming door fysieke maatregelen, zoals afgesloten containers. • Gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen • Persoonlijke aflevering. • Opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes.
10.10.1.2	Aanmaken auditlogbestanden	Een logregel bevat minimaal: • Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID. • De gebeurtenis (zie 10.10.2.1). • Waar mogelijk de identiteit van het werkstation of de locatie. • Het object waarop de handeling werd uitgevoerd. • Het resultaat van de handeling. • De datum en het tijdstip van de gebeurtenis.
10.10.1.3	Aanmaken auditlogbestanden	In een logregel wordt in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera).

BIG Nummer	titel	Genomen maatregel door Opdrachtnemer
10.10.2.1	Controle van systeemgebruik	De volgende gebeurtenissen worden in ieder geval opgenomen in de logging: • Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling: uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore. • Gebruik van functioneel beheerfuncties, zoals het wijzigingen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases). • Handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels. • Beveiligingsincidenten (zoals de aanwezigheid van malware, testen op vulnerabilities, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services). • Verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen). • Handelingen van gebruikers, zoals goede en foute inlogpogingen, systeemtoegang, gebruik van online transacties en toegang tot bestanden door systeembeheerders.
10.10.3.5	Bescherming van informatie in logestanden	De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de Opdrachtgever. Bij een (vermoed) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.
10.10.6.1	Synchronisatie van systeemklokken	Er worden maatregelen genomen om er voor te zorgen dat de logbestanden die verzameld worden aan elkaar te relateren zijn, op basis van het tijdstip waarin ze zijn opgetreden.
11.4.2.1	Authenticatie van gebruikers bij externe verbindingen.	Als externe toegang nodig is tot de persoonsgegevens van de Opdrachtgever door eigen personeel, of personeel van de Opdrachtnemer, dienen geschikte authenticatie methodes te worden gebruikt.
11.5.1.2	Beveiligde inlogprocedures	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
11.5.6.1	Beperking van verbindingstijd	De toegang voor onderhoud op afstand door een leverancier wordt alleen opengesteld op basis van een wijzigingsverzoek of storingsmelding, met 2-factor authenticatie en tunneling.
11.6.1.1	Beperking van toegang tot informatie	In de soort toegangsregels wordt ten minste onderscheid gemaakt tussen lees- en schrijfbevoegdheden.
11.6.1.2	Beperking van toegang tot informatie	Managementsoftware heeft de mogelijkheid gebruikerssessies af te sluiten.
11.6.1.3	Beperking van toegang tot informatie	Bij extern gebruik vanuit een niet vertrouwde omgeving vindt sterke authenticatie (two-factor) van gebruikers plaats.

BIG Nummer	titel	Genomen maatregel door Opdrachtnemer
12.1.1.1	Analyse en specificatie van beveiligingseisen	In projecten ten behoeve van systemen voor de Opdrachtgever wordt een beveiligingsrisicoanalyse en maatregelbepaling opgenomen als onderdeel van het ontwerp. Ook bij wijzigingen worden de veiligheidsconsequenties meegenomen.
12.2.1.1	Validatie van invoergegevens	Er moeten controles worden uitgevoerd op de invoer van gegevens. Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, toevoegen van parameters (SQL-Injectie) en inconsistentie van gegevens.
12.2.2.1	Beheersing van interne gegevensverwerking	Er bestaan voldoende mogelijkheden om reeds ingevoerde gegevens te kunnen corrigeren door er gegevens aan te kunnen toevoegen.
12.2.4.1	Validatie van uitvoergegevens	De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van de gegevens te kunnen vaststellen.
12.3.1.1	Beleid voor het gebruik van cryptografische beheersmaatregelen	De gebruikte cryptografische algoritmen voor versleuteling zijn als open standaard gedocumenteerd en zijn door onafhankelijke betrouwbare deskundigen getoetst.
12.3.2.1	Sleutelbeheer	In het sleutelbeheer is minimaal aandacht besteed aan het proces, de actoren en hun verantwoordelijkheden.
12.4.1.1	Beheersing van operationele software	Alleen geautoriseerd personeel kan functies en software installeren of activeren.
12.5.1.1	Procedures voor wijzigingsbeheer	Er is aantoonbaar wijzigingsmanagement ingericht volgens gangbare best practices, zoals ITIL en voor applicaties ASL.
12.5.2.1	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem	Van aanpassingen (zoals updates) aan softwarematige componenten van de technische infrastructuur wordt vastgesteld dat deze de juiste werking van de technische componenten niet in gevaar brengen en de beveiliging zoals afgesproken met de Opdrachtgever te niet doen.
12.5.4.2	Uitlekken van informatie	Er dient een proces te zijn om aan de Opdrachtgever te melden dat (persoons) informatie is uitgelekt. (zie 13.1.1)
12.6.1.1	Beheersing van technische kwetsbaarheden	Er is een proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat minimaal het melden van incidenten aan de Opdrachtgever, het uitvoeren van periodieke penetratietests, het uitvoeren van risicoanalyses van kwetsbaarheden en patching van systemen en hardware.
13.1.1.1	Rapportage van informatiebeveiligingsgebeurtenissen	Er is een procedure voor het rapporteren van beveiligingsgebeurtenissen aan de Opdrachtgever vastgesteld, in combinatie met een reactie- en escalatieprocedure voor incidenten, waarin de handelingen worden vastgelegd die moeten worden genomen na het ontvangen van een rapport van een beveiligingsincident.

BIG Nummer	titel	Genomen maatregel door Opdrachtnemer
13.1.1.4	Rapportage van informatiebeveiligingsgebeurtenissen	Alle beveiligingsincidenten worden vastgelegd in een systeem en geëscaleerd aan de Opdrachtgever.
13.1.1.5	Rapportage van informatiebeveiligingsgebeurtenissen	Vermissing of diefstal van apparatuur of media die gegevens van de Opdrachtgever kunnen bevatten wordt altijd ook aangemerkt als informatiebeveiligingsincident.
13.2.3.1	Verzamelen van bewijsmateriaal	Voor een vervolgprocedure naar aanleiding van een beveiligingsincident behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd in overeenstemming met de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.
15.1.3.1	Bescherming van bedrijfsdocumenten	De registraties van de Opdrachtgever behoren te worden beschermd tegen verlies, vernietiging en vervalsing, in overeenstemming met wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.
15.1.4.1	Bescherming van gegevens en geheimhouding van persoonsgegevens	De bescherming van gegevens en privacy behoort te worden bewerkstelligd in overeenstemming met relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.
15.1.6.1	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Er is vastgesteld aan welke overeenkomsten, wetten en voorschriften de toepassing van cryptografische technieken moet voldoen. Zie ook 12.3.
15.2.1.1	Naleving van beveiligingsbeleid en -normen	De Opdrachtnemer is verantwoordelijk voor uitvoering en beveiligingsprocedures en toetsing daarop (onder andere de jaarlijkse in control verklaring). Conform deze Verwerkingsovereenkomst en andere contractuele eisen zorgt de Opdrachtnemer voor het toezicht op de uitvoering van het beveiligingsbeleid ten behoeve van de gegevens van de Opdrachtgever. Daarbij behoren ook periodieke beveiligingsaudits. Deze kunnen worden uitgevoerd door, of vanwege de Opdrachtgever.
15.2.2.1	Controle op technische naleving	Informatiesystemen van de Opdrachtnemer ten behoeve van de Opdrachtgever worden regelmatig gecontroleerd op naleving van beveiligingsnormen. Dit kan door bijvoorbeeld kwetsbaarheidsanalyses en penetratietesten.

Addendum 5: Omschrijving werkzaamheden ter uitwerking van artikel 6.4

De Opdrachtnemer maakt bij de uitvoering van een Verwerkingsovereenkomst gebruik van de derden/onderaannemers die in deze bijlage zijn vermeld. De Opdrachtnemer zal deze bijlage conform artikel 6 van deze Verwerkingsovereenkomst bijwerken indien er wijzigingen plaatsvinden in de ingeschakelde derden/onderaannemers en deze lijst onverwijld ter beschikking stellen aan de verwerkingsverantwoordelijke.

Ingeschakelde derden/onderaannemers

Naam 1: HTwice	
Vestigingsplaats:	Nijmegen
Inschrijvingsnummer NHR:	57172706
Beschrijving van de werkzaamheden:	Helpdeskwerkzaamheden tbv MyExports
Voorwaarden van de verwerkingsverantwoordelijke gesteld aan toestemming:	

Naam 2: Vansimpsen ICT	
Vestigingsplaats:	Tilburg
Inschrijvingsnummer NHR:	69632863
Beschrijving van de werkzaamheden:	Helpdeskwerkzaamheden tbv MyExports
Voorwaarden van de verwerkingsverantwoordelijke gesteld aan toestemming:	

Naam 3:	
Vestigingsplaats:	
Inschrijvingsnummer NHR:	
Beschrijving van de werkzaamheden:	
Voorwaarden van de verwerkingsverantwoordelijke gesteld aan toestemming:	