Verwerkersovereenkomst

PARTIJEN:

1. U als klant, hierna te noemen **"Verwerkingsverantwoordelijke"**;
   en

2. de besloten vennootschap **Fairtual Technologies BV**, statutair gevestigd te België, 8000 Brugge, Koningin Elisabethlaan 18 en kantoorhoudende te België, 8000 Brugge, Koningin Elisabethlaan 18, in deze vertegenwoordigd door haar bestuurder, de heer Diego Dupont, hierna te noemen **"Verwerker"**.

OVERWEGINGEN:

I. Verwerkingsverantwoordelijke heeft met Verwerker een of meer overeenkomsten gesloten tot het leveren van diverse diensten door Verwerker aan Verwerkingsverantwoordelijke of zal een dergelijke overeenkomst sluiten. Deze overeenkomst of deze overeenkomsten gezamenlijk wordt of worden hierna als "**de Hoofdovereenkomst**" aangeduid.

II. Verwerker zal bij het uitvoeren van de Hoofdovereenkomst gegevens verwerken waarvoor Verwerkingsverantwoordelijke verantwoordelijk is en blijft. Tot die gegevens behoren persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming (EU 2016/679), hierna de "**AVG**".

III. Partijen willen, gelet op het bepaalde in **artikel 28 lid 3 AVG**, de voorwaarden van de verwerking van deze persoonsgegevens in deze overeenkomst vastleggen.

OVEREENKOMST:

1 Toepassingsgebied

1.1 Deze overeenkomst is van toepassing voor zover bij het leveren van de diensten onder de Hoofdovereenkomst een of meer verwerkingen plaatsvinden die zijn opgenomen in **Bijlage 1**.

1.2 De verwerkingen van **Bijlage 1** die bij het leveren van de diensten plaatsvinden worden hierna: **"de Verwerkingen"** genoemd. De persoonsgegevens die daarbij worden verwerkt: **"de Persoonsgegevens"**.

1.3 Met betrekking tot de Verwerkingen is Verwerkingsverantwoordelijke de verwerkingsverantwoordelijke en Verwerker de verwerker. De natuurlijke personen die onder de Hoofdovereenkomst feitelijk gebruik maken van de diensten van Verwerker en, eventueel, hun vertegenwoordigers, worden hierna ook als "**de Eindgebruikers**" aangeduid.

1.4 Alle begrippen in deze overeenkomst hebben de betekenis die daar in de AVG aan wordt gegeven.

1.5 De bijlagen maken onderdeel uit van deze overeenkomst. Het gaat om:

Bijlage 1 de Verwerkingen, de Persoonsgegevens en de bewaartermijnen;

Bijlage 2 de Subverwerkers en categorieën Subverwerkers die Verwerkingsverantwoordelijke goedkeurt;

Bijlage 3 de technische en organisatorische maatregelen van Verwerker;

Bijlage 4 informatie ten aanzien van een Datalek.

2 Onderwerp

2.1 Verwerker verbindt zich Persoonsgegevens uitsluitend te Verwerken ten behoeve van de in deze verwerkersovereenkomst en/of de Hoofdovereenkomst genoemde activiteiten. Verwerker garandeert dat hij, zonder uitdrukkelijke en schriftelijke toestemming van Verwerkingsverantwoordelijke, op geen enkele wijze gebruik zal maken van de Persoonsgegevens die onder deze Verwerkersovereenkomst worden Verwerkt, voor eigen doeleinden of doeleinden van derden, tenzij een op de Verwerker van toepassing zijnde wettelijke bepaling hem tot verwerking verplicht. In dat geval stelt de Verwerker de Verwerkingsverantwoordelijke, voorafgaand aan de Verwerking, onverwijld in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

2.2 Verwerker zal de Persoonsgegevens van Verwerkingsverantwoordelijke gescheiden houden van (Persoons)gegevens die zij voor zichzelf of voor derden Verwerkt.

2.3 Verwerker verricht de Verwerkingen op behoorlijke en zorgvuldige wijze.

3 Beveiligingsmaatregelen

3.1 Verwerker neemt alle technische en organisatorische beveiligingsmaatregelen die op grond van de AVG en in het bijzonder op grond van **artikel 32 AVG** van haar worden geëist.

3.2 Verwerker zal een document aanleveren waarin de passende technische en organisatorische maatregelen staan vermeld. Dit document zal als **Bijlage 3** bij deze Verwerkersovereenkomst worden gevoegd.

4 Datalekken

4.1 Verwerker zal Verwerkingsverantwoordelijke zonder onredelijke vertraging, maar in ieder geval binnen 24 uur op de hoogte stellen van iedere “inbreuk in verband met persoonsgegevens” als bedoeld in **artikel 4 sub 12 AVG**. Zo’n inbreuk wordt hierna: “**Datalek**” genoemd.

4.2 Verwerker verschaft Verwerkingsverantwoordelijke zonder onredelijke vertraging van alle informatie die zij bezit en die nodig is om aan de verplichtingen uit **artikel 33 AVG** te voldoen en zal alle door verantwoordelijke verzochte medewerking zal verlenen. Verwerker verschaft de betreffende informatie overigens zo snel mogelijk in een door Verwerker te bepalen gangbaar formaat. Verder zal Verwerker Verwerkingsverantwoordelijke op de hoogte houden van eventuele nieuwe ontwikkelingen rond het Datalek evenals alle redelijke maatregelen nemen teneinde het Datalek te verhelpen en de (mogelijke) gevolgen daarvan zo veel mogelijk te beperken. Verwerker zal tevens die maatregelen treffen die noodzakelijk zijn om een herhaling van het Datalek te voorkomen.

4.3 Verwerker stelt de Verwerkingsverantwoordelijke over een Datalek niet op de hoogte indien het volkomen duidelijk is dat dat Datalek geen enkel risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Indien er ruimte is voor twijfel daaromtrent, meldt Verwerker het Datalek wel aan de Verwerkingsverantwoordelijke teneinde deze in staat te stellen omtrent een eventuele melding van het Datalek een eigen oordeel te vormen. Verwerker zal álle inbreuken, ook die niet aan de Verwerkingsverantwoordelijke gemeld hoeven te worden, documenteren, en die documentatie eenmaal per kwartaal aan Verwerkingsverantwoordelijke verstrekken of eerder wanneer Verwerkingsverantwoordelijke daar om verzoekt. De documentatie bevat minimaal de informatie zoals bedoeld in **Bijlage 4**.

4.4 Het is uitsluitend aan Verwerkingsverantwoordelijke te bepalen of een bij Verwerker geconstateerd Datalek wordt gemeld aan de bevoegde autoriteit en/of aan betreffende betrokkenen.

5 Inschakeling Subverwerkers

5.1 Verwerker is gerechtigd bij de Verwerking derden als Subverwerker in te schakelen zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke.

5.2 Verwerker draagt er zorg voor dat de betreffende derde(n) een overeenkomst sluit(en) waarin hij zich tenminste houdt aan dezelfde wettelijke verplichtingen als die Verwerker heeft.

5.3 Verwerker licht Verwerkingsverantwoordelijke in over de door hem ingeschakelde Subverwerkers. Verwerkingsverantwoordelijke kan dan bezwaar maken tegen toevoegingen of vervangingen met betrekking tot de Subverwerkers van Verwerker.

5.4 Verwerkingsverantwoordelijke geeft hierbij in elk geval toestemming voor het inschakelen van de in **Bijlage 2** opgenomen Subverwerkers en/of categorieën van Subverwerkers.

6 Geheimhoudingsplicht

6.1 Verwerker houdt de Persoonsgegevens geheim. Verwerker draagt ervoor zorg dat de Persoonsgegevens niet direct of indirect ter beschikking komen van derden. Onder derden wordt ook het personeel van Verwerker begrepen voor zover het niet noodzakelijk is dat zij kennis nemen van de Persoonsgegevens. Dit gebod geldt niet indien in deze overeenkomst anders is bepaald en/of voor zover een wettelijk voorschrift of vonnis tot enige bekendmaking verplicht.

6.2 Verwerker draagt ervoor zorg dat personen, niet beperkt tot werknemers, die bij Verwerker deelnemen aan de Verwerkingen zijn gebonden aan een geheimhoudingsverplichting ter zake van de Persoonsgegevens.

6.3 Verwerker zal Verwerkingsverantwoordelijke op de hoogte stellen van ieder verzoek tot kennisneming, verstrekking of andere vorm van opvragen en mededeling van de Persoonsgegevens, in strijd met de in dit artikel opgenomen geheimhoudingsplicht.

7 Bewaartermijnen en wissen

7.1 Verwerkingsverantwoordelijke is verantwoordelijk voor het bepalen van de bewaartermijnen met betrekking tot de Persoonsgegevens. Voor zover Persoonsgegevens onder controle van de Verwerkingsverantwoordelijke zijn wist hij die zelf tijdig.

7.2 Verwerker zal de Persoonsgegevens binnen dertig dagen na het einde van de Hoofdovereenkomst wissen of, naar keuze van de Verwerkingsverantwoordelijke, aan deze overdragen, tenzij de Persoonsgegevens langer bewaard moeten worden, zoals in het kader van (wettelijke) verplichtingen van Verwerker, dan wel indien Verwerkingsverantwoordelijke verzoekt Persoonsgegevens langer te bewaren en Verwerker en Verwerkingsverantwoordelijke over de kosten en overige voorwaarden van dat langere bewaren overeenstemming bereiken, dit laatste onverminderd de verantwoordelijkheid van Verwerkingsverantwoordelijke de wettelijke bewaartermijnen in acht te nemen. Een eventuele overdracht aan de Verwerkingsverantwoordelijke geschiedt op kosten van de Verwerkingsverantwoordelijke.

7.3 Verwerker zal op verzoek van Verwerkingsverantwoordelijke verklaren dat het wissen in het voorgaande lid bedoeld heeft plaatsgevonden. Verwerkingsverantwoordelijke kan op eigen kosten een controle laten uitvoeren of dat inderdaad is gebeurd. **Artikel 10** van deze overeenkomst is van toepassing op die controle. Verwerker zal voor zover nodig alle Subverwerkers die betrokken zijn bij de verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Hoofdovereenkomst en zal hen instrueren te handelen zoals hierin bepaald is.

7.4 Tenzij partijen anders afspreken, draagt Verwerkingsverantwoordelijke zelf zorg voor een back up van de Persoonsgegevens.

8 Rechten van betrokkenen

8.1 Indien Verwerkingsverantwoordelijke zelf toegang heeft tot de Persoonsgegevens voldoet hij zelf aan alle verzoeken van de betrokkenen met betrekking tot de Persoonsgegevens. Verwerker zal eventueel door Verwerker ontvangen verzoeken onverwijld aan Verwerkingsverantwoordelijke doorgeven, die verantwoordelijk is voor de afhandeling van het verzoek.

8.2 Alleen voor zover het in het voorgaande lid bedoelde niet mogelijk is, zal Verwerker zijn volledige en tijdige medewerking verlenen aan Verwerkingsverantwoordelijke om:

(i) na goedkeuring van en in opdracht van Verwerkingsverantwoordelijke betrokkenen inzage te laten krijgen tot de hun betreffende Persoonsgegevens,
(ii) Persoonsgegevens te verwijderen of te corrigeren,
(iii) aan te tonen dat Persoonsgegevens verwijderd of gecorrigeerd zijn indien zij incorrect zijn (of, ingeval Verwerkingsverantwoordelijke het er niet mee eens is dat de Persoonsgegevens incorrect zijn, het feit vast te leggen dat de betrokkene zijn Persoonsgegevens als incorrect beschouwt)
(iv) de betreffende Persoonsgegevens aan Verwerkingsverantwoordelijke dan wel aan een door de Verwerkingsverantwoordelijke aangewezen derde te verstrekken in een gestructureerde, gangbare en machine leesbare vorm en
(v) Verwerkingsverantwoordelijke anderszins in de gelegenheid te stellen om aan zijn verplichtingen onder de AVG of aan andere toepasselijke wetgeving op het gebied van verwerking van de Persoonsgegevens te voldoen.

8.3 De kosten van en eisen aan de in het **voorgaande lid** genoemde medewerking stellen partijen gezamenlijk vast. Zonder een afspraak daaromtrent zijn de kosten voor de Verwerkingsverantwoordelijke.

9 Aansprakelijkheid

9.1 Verwerker is jegens Verwerkingsverantwoordelijke aansprakelijk voor alle schade en kosten die Verwerkingsverantwoordelijke lijdt als gevolg van een toerekenbare tekortkoming van Verwerker om te voldoen aan zijn verplichtingen krachtens deze overeenkomst, waaronder begrepen maar niet beperkt tot de schade die door Verwerker is veroorzaakt wanneer bij de verwerking niet is voldaan aan specifiek tot Verwerker gerichte verplichtingen van de AVG of indien in strijd met de rechtmatige instructies van Verwerkingsverantwoordelijke is gehandeld.

9.2 Verwerker vrijwaart Verwerkingsverantwoordelijke voor alle aanspraken van derden als gevolg van een toerekenbare tekortkoming van de Verwerker om zijn verplichtingen jegens Verwerkingsverantwoordelijke onder deze overeenkomst na te komen.

9.3 Onverminderd het bepaalde in dit artikel 9, geldt onverkort de in de Hoofdovereenkomst opgenomen regeling inzake aansprakelijkheid.

10 Controle

10.1 Verwerkingsverantwoordelijke heeft het recht de naleving van de bepalingen van deze overeenkomst wanneer daartoe redelijkerwijs aanleiding toe is, doch in ieder geval eenmaal per jaar, op eigen kosten te controleren of deze te laten controleren door een onafhankelijke registeraccountant of registerinformaticus.

10.2 Indien uit een dergelijke controle blijkt dat Verwerker deze overeenkomst en/of toepasselijke wettelijke bepalingen die op de Verwerking van Persoonsgegevens van toepassing zijn niet of niet behoorlijk heeft nageleefd, dient Verwerker de kosten van het onderzoek voor zijn rekening te nemen. Ook zal Verwerker onverwijld na kennisneming van de geconstateerde tekortkomingen, deze tekortkomingen herstellen. Dit onverminderd de overige rechten van Verwerkingsverantwoordelijke.

10.3 Verwerker stelt de Verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om aan te tonen dat wordt voldaan aan de verplichtingen in **artikel 28 AVG**. Indien de door de Verantwoordelijke ingeschakelde derde een instructie geeft die naar mening van de Verwerker inbreuk oplevert op de AVG dan stelt de Verwerker de Verantwoordelijke daarvan onmiddellijk in kennis.

10.4 Het onderzoek van Verwerkingsverantwoordelijke zal zich altijd beperken tot de systemen van Verwerker die voor de Verwerkingen worden gebruikt. Verwerkingsverantwoordelijke zal de bij de controle gevonden informatie geheim houden en alleen gebruiken om de naleving door Verwerker van de verplichtingen uit deze overeenkomst te controleren en de informatie of delen daarvan zo snel als kan wissen. Verwerkingsverantwoordelijke staat er voor in dat eventuele ingeschakelde derden deze verplichtingen ook op zich nemen.
Verwerker zal zelf periodieke beveiligingscontroles (laten) uitvoeren en zal jaarlijks een samenvatting verstrekken van de uitkomst van deze controle die minimaal een overzicht bevat van de risico's alsmede de maatregelen om deze te beperken en verhelpen.

11 Verwerking van Persoonsgegevens buiten de Europese Economische Ruimte

11.1 Het overbrengen van Persoonsgegevens door Verwerker buiten de Europese Economische Ruimte is alleen toegestaan met inachtneming van de daarvoor geldende wettelijke verplichtingen.

12 Overige bepalingen

12.1 Wijzigingen van deze overeenkomst zijn uitsluitend geldig indien deze tussen partijen schriftelijk zijn overeengekomen.

12.2 Partijen zullen deze overeenkomst aanpassen aan gewijzigde of aangevulde regelgeving, aanvullende instructies van de relevante autoriteiten en voortschrijdend inzicht in de toepassing van de AVG (bijvoorbeeld door, maar niet beperkt tot, jurisprudentie of rapporten), de introductie van standaardbepalingen en/of andere gebeurtenissen of inzichten die een dergelijke aanpassing nodig maken.

12.3 Deze overeenkomst duurt zolang de Hoofdovereenkomst duurt. De bepalingen van deze overeenkomst blijven gelden voor zover nodig voor de afwikkeling van deze overeenkomst en voor zover die bedoeld zijn het einde van deze overeenkomst te overleven. Tot die laatste categorie bepalingen behoren onder meer, zonder daartoe te zijn beperkt, de bepalingen omtrent geheimhouding en geschillen.

12.4 Deze overeenkomst prevaleert boven alle overige overeenkomsten tussen Verwerkingsverantwoordelijke en Verwerker.

12.5 Op deze overeenkomst is uitsluitend Belgisch recht van toepassing.

12.6 Partijen zullen hun geschillen verband houdende met deze overeenkomst uitsluitend voorleggen aan de Rechtbank Brugge.

_____	_____
Door:	Door:
Namens: **Fairtual Technologies BV**	Namens:
Op:	Op:
Te:	Te:

Bijlage 1

Verwerkingen van persoonsgegevens en bewaartermijnen

Bijlage 1 en 2 dienen door verwerkingsverantwoordelijke zo volledig mogelijk ingevuld te worden

Deze bijlage is onderdeel van de Verwerkersovereenkomst en moet door partijen geparafeerd worden.

I. De Persoonsgegevens die partijen verwachten te verwerken:

[Beschrijving van de persoonsgegevens die op grond van deze overeenkomst verwerkt worden, zoals bijvoorbeeld de hieronder omschreven gegevens. Graag aanvullen.]

- o ……
- o ……
- o ……
- o ……
- o ……
- o ……
- o ……
- o ……
- o ……
- o ……
- o ……

II. De aard, het gebruik en het doel van de verwerking van Persoonsgegevens:

[Beschrijving van wat er met de Persoonsgegevens wordt gedaan (bijvoorbeeld opslag in een bestand, e-mailing etc.), wat het doel van de verwerking is (bijvoorbeeld marketing, klantenwerving, uitvoering overeenkomst) en van welke middelen gebruik wordt gemaakt (bijvoorbeeld CRM-software).]

……
……
……
……
……
……
……
……
……

III. De categorieën van Betrokkenen waarop de Persoonsgegevens betrekking heeft

[Beschrijving van de categorieën van Betrokkenen, bijvoorbeeld bezoekers van de website, abonnees, leveranciers, kinderen, werknemers].

……
……
……
……
……
……

……
……
……

IV. De gebruiks- en bewaartermijnen van de (verschillende soorten) Persoonsgegevens:

[Beschrijving van de gebruiks- en bewaartermijnen die verwerker dient aan te houden]

……
……
……
……
……
……
……
……
……

Bijlage 2

Subverwerkers/categorieën van Subverwerkers

Deze bijlage is onderdeel van de Verwerkersovereenkomst en moet door partijen geparafeerd worden.

In deze bijlage staat een overzicht van de Subverwerkers zoals genoemd in art. 5.4 van deze overeenkomst.

Subverwerkers:

Naam subverwerker	**Adres**	**Contactgegevens**	**Doel subverwerker**
C Bloom Comm. V.	Blauwvoetstraat 49 - 8310 Assebroek	info@cbloom.be GSM:+32478211899 BE0518.858.245	3D design
Sliced Comm. V.	Watermolenstraat 23 9230 Wetteren	info@sliced.be GSM:+32496660979 BE0739734272	IT - development
Combell NV	Skaldenstraat 121, 9042 Gent	administratie@combell.com BTW: BE 0541.977.701	hosting
Whereby AS	Gate 1, N° 107 6700 Maloy, Norway	pro@whereby.com	Video meetings
tawk.to inc.	187 East Warm Springs Rd, SB298 Las Vegas, NV, 89119	support@tawk.to	Written chat booths
Chatwee Sp.	Piotrkowska 4, 62-610 Sompolno, Polnad	VAT ID: PL6652990463 https://chatwee.com/	Written Chat (Network Café)

Hoofdstuk	Onderwerp	Status
Beveiligingsbeleid en organisatie van informatiebeveiliging	Gegevensbescherming: Er werd een DPO aangesteld die verantwoordelijk is voor het coördineren, adviseren, controleren en sensibiliseren van procedures en richtlijnen omtrent gegevensbescherming. Deze verantwoordelijke zal periodiek worden bijgeschoold zodat zijn kennis en deskundigheid steeds actueel blijft.	Er is een DPO aangeduid die beschikt over de nodige competenties om zijn opdracht uit te voeren. De DPO heeft een duidelijke functieomschrijving en er kunnen geen belangenconflicten ontstaan door andere taken die de DPO uitvoert binnen de organisatie. Er zijn voldoende middelen voorhanden en er wordt voldoende tijd gespendeerd aan de organisatie van informatieveiligheid met betrekking tot de verwerking van persoonsgegevens. Er bestaat een actief beslissingsplatform (DPO + projectteam) dat op regelmatige basis vergadert en beslissingen neemt. Er bestaat eveneens een duidelijke ondersteuning van de directie om de implementatie van de gegevensbescherming in de organisatie op te starten, te beheersen, te onderhouden en waar nodig bij te sturen.
	Beveiligingsverantwoordelijkheden: Er zijn formele beleidsteksten omtrent gegevensbescherming goedgekeurd en bekend onder de medewerkers. De verantwoordelijkheden omtrent gegevensbescherming zijn intern toebedeeld.	Er bestaat een algemeen informatieveiligheidsbeleid met betrekking tot de verwerking van persoonsgegevens, die zowel intern als extern werd / wordt gecommuniceerd en dat regelmatig wordt geëvalueerd. Er bestaat een actieve ondersteuning vanuit de directie naar de freelancers met wie wordt samengewerkt met betrekking tot de naleving van het algemeen informatieveiligheidsbeleid met betrekking tot de verwerking van persoonsgegevens.
	Risicobeheer: Er werd een formele risicoanalyse uitgevoerd waaruit maatregelen ten aanzien van gegevensbescherming werden opgesteld. Dit proces zal periodiek worden herhaald.	Er werd en er wordt op regelmatige basis een risicoanalyse uitgevoerd om te beoordelen wat de risico zijn bij verlies, onrechtmatige overdracht, wijziging… van persoonsgegevens. Er werd en wordt op regelmatige basis een afweging gemaakt tussen de kostprijs voor het nemen van technische en organisatorische maatregelen t.o.v. de risico's van eventuele inbreuken en de gevolgen ervan voor de rechten en vrijheden van betrokkenen. Er werden en worden regelmatig technische en organisatorische maatregelen genomen om risico's te vermijden die een invloed kunnen hebben op de rechten en vrijheden van betrokkenen.
Veilig personeelsbeleid	Vertrouwelijkheidsverplichtingen: De medewerkers zijn onderworpen aan een vertrouwelijkheidsverplichting bij het verwerken van persoonsgegevens. Deze verplichting is opgenomen in de arbeidsovereenkomst of in het arbeidsreglement.	De Verwerker heeft geen personeel in dienst. Met alle freelancers werd een vertrouwelijkheidsovereenkomst afgesloten. Er bestaan interne disciplinaire maatregelen voor overtredingen die betrekking hebben op de omgang met persoonsgegevens. Er wordt op regelmatige basis gecontroleerd op welke manier medewerkers met persoonsgegevens omgaan.
	Sensibilisering: De medewerkers zijn zich bewust van het belang van gegevensbescherming en zullen de nodige procedures volgen bij de verwerking van persoonsgegevens. Deze sensibilisering zal periodiek worden herhaald	Elke freelancer die met de Verwerker samenwerkt heeft diverse awareness-trainingen gevolgd zowel op het gebied van GDPR als op het gebied van cyber security.
	In- en uitdiensttreding: De toegangsrechten van de verschillende werknemers worden bij de beëindiging van de samenwerking stopgezet zodat onbevoegden geen toegang meer hebben tot de persoonsgegevens.	Er wordt rekening gehouden bij interne verschuivingen van medewerkers die persoonsgegevens verwerken of zullen verwerken. Toegangsrechten en andere rechten worden desgevallend geëvalueerd en aangepast.
Inventaris van bedrijfsmiddelen	Inventaris van bedrijfsmiddelen: Er wordt een inventaris bijgehouden van alle informatie verwerkende systemen die worden gebruikt door de werknemers.	Er wordt op organisatieniveau een duidelijk onderscheid gemaakt tussen persoonsgegevens, anonieme gegevens, gecodeerde gegevens en gevoelige gegevens.

Cryptografie	Bedrijfsmiddelen: Alle informatie verwerkende systemen waarop informatie van de verwerkingsverantwoordelijke worden verwerkt zijn passend geëncrypteerd.	Er bestaat een beleid omtrent gebruik van encryptie dat wordt afgestemd met de risicoanalyse om de vertrouwelijkheid, authenticiteit en/of integriteit van persoonsgegevens te beschermen. De organisatie heeft een beleid ontwikkeld voor de bescherming van de levensduur van cryptografische sleutels tijdens hun gehele levenscyclus.
	Informatietransfers: Alle vertrouwelijke gegevens van de verwerkingsverantwoordelijke worden enkel getransfereerd met behulp van een beveiligde verbinding.	Er wordt steeds gebruik gemaakt van beveiligde verbindingen.
Fysieke beveiliging	Fysieke toegang: Toegang tot de gebouwen waar persoonsgegevens worden verwerkt is enkel toegankelijk voor geïdentificeerde en geautoriseerde personen.	Er worden gepaste beveiligingsmaatregelen genomen inzake fysieke beveiliging van lokalen en gebouwen. Er wordt rekening gehouden met elke potentiële vorm van schade (brand, water…). Er wordt rekening gehouden met de beveiliging van apparatuur, bekabeling en de ondersteunende voorzieningen om verlies, schade, diefstal en het ongewenst veranderen van persoonsgegevens te voorkomen. Er wordt bijzondere aandacht besteed aan apparatuur die zich buiten het terrein van de organisatie bevindt of wordt gebruikt.
Toegangscontrole	Toegangsbeleid: De rechten van iedere werknemer zullen beperkt worden volgens het 'need-to-know' principe. Meer toegang dan initieel noodzakelijk zal enkel mogelijk zijn naar een formele goedkeuring en bij de aanwezigheid van een geldige reden.	Er bestaat een actueel en gedocumenteerd toegangsbeleid waarbij duidelijk is wie toegang heeft tot welke persoonsgegevens. Hier wordt rekening gehouden met Dataclassificatie. Er is een verantwoordelijke aangesteld voor de aanvragen met betrekking tot de toegangsrechten. Deze verantwoordelijke is verschillend van de persoon die de toegangsrechten op technisch niveau in de systemen toekent, aanpast of verwijdert. Er bestaan passende beveiligingsmaatregelen omtrent toegang tot data (zoals paswoordbeveiliging). Er bestaat functiescheiding om te verhinderen dat één persoon alle rechten heeft.
	Toegangsautorisatie: Om toegang te krijgen tot gevoelige informatie is er een passend autorisatiesysteem. Ieder individu zal een unieke ID krijgen waarmee hij kan inloggen.	
	Authenticatie: Voor de authenticatie van gebruikers is er een sterk authenticatiesysteem geïmplementeerd. Indien toegang tot gevoelige persoonsgegevens via internet mogelijk is moet er gebruik worden gemaakt van multi-factor authenticatie.	
	Netwerktoegang: Er is een systeem aanwezig die een redelijke mate van zekerheid biedt dat toegang tot het netwerk gepast wordt beschermd (bv. firewalls, securityvoorzieningen,…)	Netwerkbeveiliging (firewall, WiFi…) maakt onderdeel uit van het informatieveiligheidsplan.
Operationele beveiliging	Back-up: Er worden op periodieke basis back-ups genomen van de persoonsgegevens. Deze back-ups zullen geëncrypteerd worden bewaard op een externe locatie.	Er bestaat een geschikt back-up beleid, welke regelmatig wordt getest en opgevolgd om een adequaat herstel te waarborgen na schade, verlies, diefstal en ongewenste wijziging van persoonsgegevens. Er bestaat een beleid omtrent gebruik van encryptie dat wordt afgestemd met de risicoanalyse om de vertrouwelijkheid, authenticiteit en/of integriteit van persoonsgegevens te beschermen. De organisatie heeft een beleid ontwikkeld voor de bescherming van de levensduur van cryptografische sleutels tijdens hun gehele levenscyclus.
	Beveiligingsupdates: Beveiligingsupdates en -patches worden systematisch opgevolgd en geïnstalleerd.	Er bestaat geüpdatete bescherming tegen malware. Er heerst voldoende bewustzijn bij de systeem- en de eindgebruikers. Beveiligingsupdates worden regelmatig uitgevoerd.
Communicatie-beveiliging	Transfer over netwerken: Alle persoonsgegevens die worden verzonden via publieke of interne kanalen of netwerken zullen adequaat worden versleuteld.	Er bestaat een e-mail- en internetbeleid (transport), waarbij men bijzondere aandacht besteedt aan het gebruik van persoonsgegevens in e-mail.
Leveranciers-relaties	Keuze van Subverwerkers/onderaannemers: Er wordt een adequaat selectieproces gehanteerd bij de keuze van Subverwerkers/onderaannemers waarbij de beveiliging van persoonsgegevens wordt geëvalueerd. Enkel partijen die voldoen aan de huidige standaarden op vlak van informatieveiligheid en	De beveiligingsinspanningen van de informatiesystemen van de subverwerkers / onderaannemers worden bij aanschaf gecontroleerd. Ook bij de ontwikkeling van nieuwe informatiesystemen of bij uitbreidingen van bestaande informatiesystemen (toepassingen, diensten, IT-middelen of andere informatie verwerkende onderdelen…) wordt er controle uitgeoefend op de beveiligingseisen.

	gegevensbescherming zullen worden gebruikt voor de verwerking van persoonsgegevens.	
	Contractuele verplichtingen: Er is een verwerkersovereenkomst aanwezig met alle mogelijke leveranciers die persoonsgegevens zullen verwerken. Deze overeenkomst bevat alle verplichte bepalingen en werd ondertekend.	Er zijn juridisch goedgekeurde verwerkersovereenkomsten voorhanden met externe verwerkers. Verwerkersovereenkomsten worden gecheckt op beveiliging van persoonsgegevens. De verwerkersovereenkomsten bevatten voldoende garanties dat de (sub)verwerker(s) persoonsgegevens verwerken dit doen conform de AVG. Er wordt controle uitgeoefend op deze (sub)verwerker(s) teneinde de conformiteit aan de AVG te waarborgen.
Beheer van informatie-beveiligings-incidenten	Incident management: Er is een interne procedure die garandeert dat mogelijke beveiligingsinbreuken ook worden gemeld en vervolgens worden afgehandeld door de verantwoordelijken. Deze procedure werd ook duidelijk intern gecommuniceerd. Alle mogelijke beveiligingsinbreuken worden op een centrale plaats verzamelt.	Er wordt voor gezorgd dat aan de hand van gedocumenteerde procedures kan gedetecteerd, gehandeld en gerapporteerd worden inzake incidenten. Bij incidenten wordt de DPO onmiddellijk op de hoogte gebracht. De DPO kent alle zwakke plekken die kunnen leiden tot incidenten, alsook de oplossingen die risico's kunnen vermijden. Bij een voorkomend incident liggen de verantwoordelijkheden vast.
	Notificatie van incidenten: Bij een mogelijk beveiligingsincident dat een impact heeft op de vertrouwelijkheid, integriteit of beschikbaarheid van persoonsgegevens zullen de nodige stappen worden ondernomen om de verwerkingsverantwoordelijke tijdig en voldoende in te lichten hierover.	De organisatie is in staat de continuïteit en de beschikbaarheid van de persoonsgegevens steeds te waarborgen op basis van de resultaten van een risicoanalyse. Er bestaat een bedrijfscontinuïteitsplan. De organisatie voorziet voldoende redundantie (= het voorkomen van iets) binnen de gegevensverwerkende diensten om de beschikbaarheid van persoonsgegevens te waarborgen. Bijkomende gegevensbeschermingsrisico's als gevolg van redundantie worden hierbij in acht genomen.
Bedrijfscontinuïteit	Noodherstel: Er is een gepast systeem aanwezig om in geval van storingen de beschikbaarheid en integriteit van gegevens te garanderen	Er bestaat een privacyverklaring die voldoet aan AVG en volgende gegevens bevat: • De identiteit van de verwerkingsverantwoordelijke • De doeleinden waarvoor de gegevens zullen worden verwerkt • De persoonsgegevens die per doeleinde worden verwerkt • De wettelijke grondslag voor gegevensverwerking • De bewaartermijnen • Of de gegevens uitgewisseld worden buiten de Europese Unie • De mogelijkheid voor de betrokkene om een klacht in te dienen bij de GBA indien hij/zij meent dat zijn/haar persoonsgegevens foutief worden verwerkt • De rechten voor de betrokkenen • De technische en organisatorische maatregelen die de organisatie neemt ter bescherming van de persoonsgegevens Er bestaat een register van verwerkingsactiviteiten dat voldoet aan de AVG wetgeving. Dit register bevat: • de naam en contactgegevens van de (gezamenlijke) verwerkingsverantwoordelijke, van de vertegenwoordiger van de verwerkingsverantwoordelijke en/of van de functionaris voor gegevensbescherming • de verwerkingsdoeleinden • een beschrijving van de categorieën van betrokkenen • een beschrijving van de categorieën van persoonsgegevens? • de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt • de ontvangers in derde landen of internationale organisaties • de bewaartermijnen • een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen? • doorgiften van persoonsgegevens aan een derde land of een internationale organisatie en indien nodig de documenten inzake de passende waarborgen? Er kan voldaan worden aan verzoeken van betrokkenen met betrekking tot hun rechten: • De rechten van betrokkenen worden in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ter beschikking gesteld van betrokkenen? • De organisatie komt tegemoet aan het recht op informatie. • De organisatie komt tegemoet aan het recht van inzage.

		• De organisatie komt tegemoet aan het recht op correctie. • De organisatie komt tegemoet aan het recht op verwijdering / recht op vergetelheid. • De organisatie komt tegemoet aan het feit dat de draagwijdte van de verwerkte persoonsgegevens beperkt is. • De organisatie houdt rekening met het recht op overdraagbaarheid van gegevens. • De organisatie komt tegemoet aan het recht van bezwaar. • De organisatie houdt rekening met het recht van de betrokkene om niet aan geautomatiseerde besluitvorming, waaronder profiling, onderhevig te zijn De organisatie heeft de wettelijke grondslagen voor elke verwerking gedefinieerd. Er wordt, indien nodig, toestemming gevraagd aan de betrokken voor de verwerking van hun persoonsgegevens, waarbij een vrijwillige keuze wordt voorzien waarbij betrokken uitdrukkelijk kan instemmen (een opt-in). De toestemming wordt middels een actieve handeling verkregen en de betrokkene kan te allen tijde zijn / haar toestemming intrekken op een even eenvoudige manier als de opt-in werd voorzien. Alle verkregen toestemmingen tot verwerking van persoonsgegevens zijn controleerbaar (logging…). Er worden geen gegevens van kinderen verwerkt. Voorafgaand aan alle verwerkingen werd een DPIA of een Gegevensbeschermingseffectbeoordeling uitgevoerd wanneer er een groot privacy risico blijkt. De organisatie volgt de wetgeving en rechtspraak inzake de AVG op regelmatige tijdstippen op.
Naleving	Compliance: De aantoonbaarheid rond de eisen van naleving kan opgevraagd worden door de verwerkingsverantwoordelijke	

Bijlage 4

Informatie ten aan zien van een Datalek

Verwerker zal alle inlichtingen verschaffen die Verwerkingsverantwoordelijke noodzakelijk acht om het Datalek of incident te kunnen beoordelen. Daarbij verschaft Verwerker in ieder geval de volgende informatie aan Verwerkingsverantwoordelijke:

- wat de (vermeende) oorzaak is van het Datalek of incident;
- wat het (vooralsnog bekende en/of te verwachten) gevolg is;
- wat de voorgestelde oplossing is;
- de contactgegevens voor de opvolging van de melding;
- (een inschatting van) het aantal personen waarvan gegevens betrokken zijn bij het Datalek of incident;
- een omschrijving van de categorie betrokkenen die betrokken zijn bij het Datalek of incident;
- het soort of de soorten Persoonsgegevens die betrokken zijn bij het Datalek of incident;
- de datum waarop/periode waarin het Datalek of incident heeft plaatsgevonden;
- de datum en het tijdstip waarop het Datalek of incident bekend is geworden bij Verwerker of bij een door hem ingeschakelde derde of sub verwerker;
- of de gegevens versleuteld, gehasht of op een andere manier ontoegankelijk zijn gemaakt voor onbevoegden;
- wat de genomen maatregelen zijn om het Datalek of incident te beëindigen en om de gevolgen van de inbreuk te beperken.