FAIRTUAL
TECHNOLOGIES BV

Verwerkersovereenkomst cfr. Art. 28 AVG

Vanaf 01-01-2021

Tussen u (als Verwerkingsverantwoordelijke) en ons (als Verwerker), samen "De Partijen" en overwegende dat:

(a) Verwerkingsverantwoordelijke (verder: u) en de Verwerker (verder: wij) vanaf 25 mei 2018 onderworpen zijn aan de Algemene Verordening Gegevensbescherming ('AVG').

(b) Verwerkingsverantwoordelijke (verder: u) en de Verwerker (verder: wij) zijn verbonden door een contractuele relatie (hierna het 'Contract) waarbij wij als Verwerker van Persoonsgegevens, in opdracht van u als Verwerkingsverantwoordelijke optreden.

(c) In het kader van onze contractuele relatie, wensen Verwerkingsverantwoordelijke (verder: u) en Verwerker (verder: wij) deze Verwerkersovereenkomst onze respectievelijke rechten en plichten te regelen inzake de Verwerking van Persoonsgegevens.

Wordt overeengekomen wat volgt

De in deze Overeenkomst in hoofdletter geschreven woorden zijn afkortingen, begrippen en verduidelijkingen die voor deze Overeenkomst de volgende betekenis hebben:

- **AVG**: De Algemene Verordening Gegevensbescherming, met name de verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 96/46/EG, met haar wijzigingen en Europese uitvoeringswetgeving.

- **Persoonsgegevens**, Verwerking, Verwerkingsverantwoordelijke, Verwerker, Betrokkene, Derde, Toezichthoudende autoriteit: de begripsomschrijvingen zoals bepaald in de Algemene Verordening Gegevensbescherming.

- **Inbreuk in verband met Persoonsgegevens**: Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens.

- **Subverwerker**: Een natuurlijke persoon of rechtspersoon die rechtstreeks of onrechtstreeks onder de verantwoordelijkheid werkt van de Verwerker (wij), met uitzondering van personen die in dienstverband voor de Verwerker (wij) werken.

- **Toepasselijke Wetgeving**: De Algemene Verordening Gegevensbescherming, andere Europese regelgeving waarin bepalingen met betrekking tot gegevensbescherming en privacy worden opgenomen, evenals de toepasselijke nationale wetgeving inzake gegevensbescherming en privacy in de lidstaten met haar wijzigingen en uitvoeringsbesluiten, met inbegrip van voor de sector toepasselijke goedgekeurde gedragscodes.

FAIRTUAL
TECHNOLOGIES BV

Artikel 1. Toepassingsgebied

1.1. Deze overeenkomst is opgesteld in het kader van de Algemene Verordening Gegevensbescherming, met name de verordening 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van Persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EC.

1.2. De bepalingen uit de Verwerkersovereenkomst zijn onverkort van toepassing op alle Verwerkingen van Persoonsgegevens die wij verrichten in het kader van de uitvoering van de verwerkingsactiviteiten bepaald in Bijlage 1 van de Verwerkersovereenkomst.

Artikel 2. Schriftelijke instructies van u

2.1 Bij de Verwerking van Persoonsgegevens handelen de Partijen in overeenstemming met de Toepasselijke Wetgeving.

2.2 Wij wenden de Persoonsgegevens enkel aan voor de uitvoering van onze verplichtingen in overeenstemming met de Verwerkersovereenkomst en volgens uw schriftelijke instructies als Verwerkingsverantwoordelijke. De schriftelijke instructies worden opgenomen in Bijlage 1 van de Verwerkersovereenkomst. Indien de schriftelijke instructies niet duidelijk zijn, melden wij dit schriftelijk aan u waarop in onderling overleg de instructies zullen worden verduidelijkt.

2.3 Behoudens andersluidende bepalingen in de Verwerkersovereenkomst zullen wij de Persoonsgegevens (i) niet gebruiken voor eigen doeleinden, (ii) niet doorsturen naar een land gelegen buiten de Europese Economische Ruimte, zonder daartoe een schriftelijke instructie te hebben ontvangen van u.

2.4 Indien Europese of nationale regelgeving ons (wij) tot een bepaalde Verwerking verplicht, stellen wij u, voorafgaand aan de Verwerking, in kennis van dat wettelijk voorschrift, tenzij die regelgeving deze kennisgeving om gewichtige reden van algemeen belang verbiedt.

2.5 U geeft instructies aan ons in overeenstemming met de Toepasselijke Wetgeving en waarborgt dat alle Persoonsgegevens die aan ons worden toevertrouwd rechtmatig werden verkregen en kunnen worden verwerkt in het kader van de Hoofdovereenkomst.

2.6 Wij stellen u onmiddellijk in kennis indien naar onze mening een instructie een inbreuk oplevert op de Toepasselijke Wetgeving.

Artikel 3. Technische en organisatorische beveiligingsmaatregelen

3.1 Wij treffen passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen.

3.2 Bij het bepalen van de maatregelen wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen. De maatregelen omvatten, waar passend, onder meer het volgende:

a) Pseudonimisering en versleuteling van Persoonsgegevens;

b) Het vermogen om op permanente basis de vertrouwelijkheid, integriteit en veerkracht van de verwerkingssystemen en diensten te garanderen;

c) Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de Persoonsgegevens tijdig te herstellen;

d) Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de Verwerking.

3.3 Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

3.4 Wij zullen ons richten naar de normen van gedragscodes en certificeringsmechanismen zoals die gelden binnen de sector die op de Partijen van toepassing zijn. Deze gedragscodes en certificeringsmechanismen zullen onder geen enkel beding van kracht gaan voor de goedkeuring door de toezichthoudende autoriteit.

3.5 Wij verbinden ons er toe de passende technische en organisatorische maatregelen die door ons worden getroffen op te sommen in Bijlage 2 van deze Verwerkersovereenkomst. Wij rapporteren op eigen initiatief a de wijzigingen an u die aan de maatregelen worden doorgevoerd en dit binnen een termijn van veertien dagen na het aanbrengen van de wijzigingen.

3.6 Op vraag van u beantwoorden wij alle vragen met betrekking tot de genomen technische en organisatorische maatregelen die van toepassing zijn op de verwerkte of te verwerken gegevens. Verder zullen wij op eenvoudig verzoek van u bewijs voorleggen dat de gepaste technische en organisatorische maatregelen effectief zijn genomen.

Artikel 4. Verwerking door Subverwerkers en werknemers

4.1 Wij waarborgen dat de bepalingen van de Verwerkersovereenkomst worden nageleefd door onze werknemers, vertegenwoordigers, agenten en onderaannemers. Wij waarborgen dat de tot het verwerken van Persoonsgegevens gemachtigde personen zich contractueel ertoe hebben verbonden om de vertrouwelijkheid in acht te nemen dan wel door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden. Wij maken ons sterk dat elke Subverwerker die wij toegang geven tot de Persoonsgegevens de bepalingen van deze Verwerkersovereenkomst zal naleven.

4.2 Wij zijn niet gerechtigd bij de Verwerking van de Persoonsgegevens een Derde in te schakelen zonder de voorafgaande specifieke of algemene schriftelijke toestemming van u:

a) In geval van een specifieke schriftelijke toestemming moeten wij, voorafgaandelijk aan de Verwerking van Persoonsgegevens, de toestemming verkrijgen van u voor de Verwerking van Persoonsgegevens door de Subverwerker.

b) In geval van een algemene schriftelijke toestemming, schakelen wij enkel een Derde als Subverwerker in voor zover wij u tijdig en in ieder geval voorafgaand over de identiteit van de Subverwerker hebben ingelicht en voor zover u zich hiertegen niet heeft verzet.

4.3 Indien wij een beroep doen op een Subverwerker, garanderen wij dat deze contractueel onderworpen wordt aan minstens dezelfde verplichtingen als deze waartoe wij zijn gehouden ten aanzien van u onder deze Verwerkersovereenkomst.

4.4 Wanneer wij verwerkingsactiviteiten van Persoonsgegevens toevertrouwen aan Subverwerkers zullen wij ten aanzien van u volledig aansprakelijk blijven voor het nakomen van de verplichtingen van de Subverwerker.

Artikel 5. Bijstand met betrekking tot het gegevensbeschermingsbeleid

5.1 Rekening houdend met de aard van de Verwerking en de ons ter beschikking staande informatie, verbinden wij ons ertoe bijstand te verlenen aan u bij het naleven van de uw wettelijke verantwoordelijkheid als Verwerkingsverantwoordelijke om volgende verplichtingen in het kader van gegevensbescherming na te leven:

a) Het treffen van passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen;

b) Het melden van een Inbreuk in verband met Persoonsgegevens aan de toezichthoudende autoriteit;

c) Het melden van een Inbreuk in verband met Persoonsgegevens aan de Betrokkene;

d) Het uitvoeren van een gegevensbeschermingseffectbeoordeling;

e) Het voorafgaand raadplegen van de toezichthoudende autoriteit indien uit de gegevensbeschermingseffectbeoordeling blijkt dat de Verwerking een hoog risico zou opleveren indien u geen maatregelen neemt om het risico te beperken.

5.2 De tijd en middelen die wij spenderen voor het verlenen van de bijstand, zijn voor eigen rekening van ons.

5.3 In het verlengde van artikel 5.1, lichten wij u omstandig en onmiddellijk in over een (vermoedelijke) Inbreuk in verband met Persoonsgegevens alsook over ieder gegevenslek (ook bij de Subverwerker) zodra wij hiervan kennis hebben genomen. De kennisgeving gebeurt op een dergelijke wijze dat u tijdig kan voldoen aan uw wettelijke verplichtingen als verwerkingsverantwoordelijke onder de Toepasselijke Wetgeving.

5.4 Wij leveren tevens bijstand in het onderzoek naar en de beperking en remediëring van een Inbreuk in verband met Persoonsgegevens. Daarbij zullen wij onder meer ook bijstand verlenen met het oog op het documenteren van maatregelen ter ondersteuning van de melding van de inbreuk en om de gevolgen van een inbreuk in te schatten en te beperken.

5.5 Wij stellen u onmiddellijk in kennis van enige gemaakte klacht, beschuldiging of aanvraag met betrekking tot de Verwerking van Persoonsgegevens. Wij bieden alle nodige medewerking en ondersteuning die u redelijkerwijze kan verwachten met betrekking tot dergelijke klacht, beschuldiging of aanvraag, onder meer door volledige informatie te verstrekken over dergelijke klacht, beschuldiging of aanvraag.

Artikel 6. Bijstand met betrekking tot de verzoeken van de Betrokkene

6.1 Wij zullen elk verzoek of vraag die wij van een Betrokkene ontvangen in verband met de (Verwerking van) Persoonsgegevens onverwijld doorgeven aan u, die beslist welke gevolgen hieraan zullen worden gegeven. Wij behandelen de verzoeken en aanvragen van de Betrokkenen niet zelf, behoudens eventuele andersluidende schriftelijke afspraken tussen u en ons.

6.2 Rekening houdend met de aard van de Verwerking, verlenen wij u door middel van passende technische en organisatorische maatregelen bijstand bij het vervullen van de uw plicht om verzoeken tot uitoefening van de rechten van de Betrokkene, zoals bepaald in de Toepasselijke Wetgeving, te beantwoorden. Dit impliceert onder meer:

a) Dat wij alle door u opgevraagde Persoonsgegevens bezorgen, binnen de door de u verzochte (redelijke) tijdsspanne, in ieder geval met inbegrip van de volledige details en kopieën van de klacht, mededeling of aanvraag en enige Persoonsgegevens in zijn bezit met betrekking tot een Betrokkene;

b) Dat wij zulke technische en organisatorische maatregelen implementeren die u toelaten doeltreffend en tijdig te antwoorden op relevante klachten, mededelingen of aanvragen.

6.3 De tijd en middelen die wij spenderen voor het verlenen van de bijstand, zijn voor eigen rekening van ons.

6.4 In het verlengde van artikel 6.2 verbinden wij ons ertoe u onverwijld in te lichten indien wij van een Betrokkene een van de volgende verzoeken krijgen:

a) Een aanvraag tot inzage tot de Persoonsgegevens die van de Betrokkene worden verwerkt;

b) Een aanvraag tot rectificatie van onjuiste Persoonsgegevens;

c) Een aanvraag tot wissing van Persoonsgegevens;

d) Een aanvraag tot beperking van de Verwerking van Persoonsgegevens;

e) Een aanvraag tot het verkrijgen van een draagbare kopie van de Persoonsgegevens, of tot overdracht van een kopie aan een Derde;

f) Een bezwaar tegen enige Verwerking van Persoonsgegevens; of

g) Elke andere aanvraag, klacht of mededeling met betrekking tot uw verplichtingen onder de Toepasselijke Wetgeving.

Artikel 7. Recht op controle

7.1 U heeft steeds het recht om de naleving door ons van de Verwerkersovereenkomst te controleren. Wij stellen u alle informatie ter beschikking die nodig is om de nakoming van de verplichtingen in het kader van de Toepasselijke Wetgeving aan te tonen.

7.2 U heeft de mogelijkheid om een onafhankelijke audit te laten uitvoeren door een onafhankelijke derde die door u wordt aangeduid. Wij kunnen redelijke bezwaren laten gelden met betrekking tot deze derde.

7.3 Deze audit zal op kosten van u geschieden en zal de normale werking van ons niet storen. De door u aangestelde auditor zal vooraf een vertrouwelijkheidsovereenkomst met ons ondertekenen. Het door hem te voeren onderzoek en op te stellen verslag zal enkel betrekking hebben op het nazicht van de naleving van passende technische en organisatorische maatregelen die nodig zijn om de nakoming van de verplichtingen in het kader van de Toepasselijke Wetgeving en onderhavige Verwerkersovereenkomst te waarborgen.

7.4 Wij zullen aan de aangestelde auditor eveneens inzage verlenen in de overeenkomsten die wij hebben gesloten met alle Subverwerkers die betrokken zijn bij de Verwerking van Persoonsgegevens.

7.5 Wij verlenen volledige medewerking met betrekking tot een dergelijke audit en leveren, op uw vraag, het bewijs van de naleving van onze verplichtingen onder de Verwerkersovereenkomst.

Artikel 8. Functionaris voor de gegevensbescherming

8.1 Wij zullen conform artikel 37 AVG handelen wat betreft het aanstellen van een functionaris voor de gegevensbescherming.

8.2 Wij zullen de identiteit- en contactgegevens van de functionaris voor de gegevensbescherming bezorgen aan u door middel van Bijlage 1 van de Verwerkersovereenkomst. Indien tijdens de duurtijd van deze Overeenkomst er een andere functionaris voor de gegevensbescherming wordt aangesteld, brengen wij u hiervan onmiddellijk op de hoogte.

Artikel 9. Aansprakelijkheid

9.1 De in dit artikel geregelde aansprakelijkheid heeft uitsluitend betrekking op de eventuele aansprakelijkheid ten gevolge van een inbreuk op de Toepasselijke Wetgeving inzake gegevensbescherming en/of op deze Verwerkersovereenkomst.

9.2 Wij zijn aansprakelijk ten aanzien van u voor schade die door Verwerking is veroorzaakt wanneer bij de Verwerking niet is voldaan aan de specifiek tot verwerkers gerichte verplichtingen van de GDPR, dan wel uit een handeling of nalatigheid in strijd met de rechtmatige instructies van u.

Artikel 10. Duur en Beëindiging

10.1 Deze Verwerkersovereenkomst treedt in werking op datum van ondertekening / aanvaarding.

10.2 Deze Verwerkersovereenkomst blijft van kracht zolang het Contract van kracht blijft. Indien het Contract een einde neemt, dan wordt deze Verwerkersovereenkomst eveneens beëindigd.

10.3 Na de beëindiging van deze Verwerkersovereenkomst zullen wij, naargelang de uw keuze, alle Persoonsgegevens wissen of deze terug aan u bezorgen, en bestaande kopieën ervan verwijderen, tenzij opslag van de Persoonsgegevens verplicht is op basis van een Unierechtelijke of nationaalrechtelijke regelgeving.

Artikel 11. Diverse bepalingen

11.1 Deze Verwerkersovereenkomst is deelbaar. Indien één of meer bepalingen die niet de essentie van de Verwerkersovereenkomst aanbelangen, geheel of gedeeltelijk ongeldig, nietig of onuitvoerbaar worden verklaard, dan zal dit de geldigheid en uitvoerbaarheid van de overige bepalingen niet aantasten. De Verwerkersovereenkomst zal in dat geval blijven bestaan tussen de Verwerker en de Verwerkingsverantwoordelijke. De ongeldig, nietig of onuitvoerbaar verklaarde bepaling zal dan als niet geschreven worden beschouwd. De Partijen zullen onderhandelingen aanknopen en de kwestieuze bepaling vervangen door een rechtsgeldige bepaling die de oorspronkelijke bepaling zo dicht als mogelijk benadert.

11.2 De Verwerkersovereenkomst kan alleen gewijzigd worden door middel van een schriftelijke overeenkomst tussen de Partijen.

11.3 Deze Verwerkersovereenkomst wordt geregeld door en uitgelegd in overeenstemming met het Belgisch recht. Alle geschillen die voortvloeien uit deze Verwerkersovereenkomst behoren uitsluitend tot de bevoegdheid van de hoven en rechtbanken van het gerechtelijk arrondissement waar de Verwerkingsverantwoordelijke zijn maatschappelijke zetel zich bevindt.

BIJLAGE 1: VERWERKINGSOPDRACHT EN INSTRUCTIES BETREFFENDE DE VERWERKING VAN PERSOONSGEGEVENS VAN DE VERWERKINGSVERANTWOORDELIJKE

In deze Bijlage worden de specifieke verwerkingen door de Verwerker (verder: wij of ons) beschreven waartoe de Verwerkingsverantwoordelijke (verder: u of uw) opdracht geeft op het ogenblik van het sluiten van

het Contract. Wijzigingen en/of aanvullingen van deze Bijlage gebeuren telkens via een afzonderlijk document als bijvoegsel bij deze Bijlage. Verwerkingsverantwoordelijke en Verwerker worden verder als "de Partijen" vermeld.

1. Het doel van de verwerking van persoonsgegevens

De verwerking van persoonsgegevens door ons gebeurt in het kader van de uitvoering van het Contract inzake een virtueel evenement, dat omschreven wordt in een tussen Partijen opgestelde en goedgekeurde offerte (het Contract), waarvan de Algemene Voorwaarden in haar totaliteit worden of werden aanvaard.

Beschrijving van de diensten onder het Contract en van de aard en het doel van de verwerking van persoonsgegevens in het kader van de diensten:

• Wij stellen virtueel platform ter beschikking van u gedurende een overeengekomen periode en dit op een overeengekomen URL.

• Doel van dit virtueel platform is bezoekers, exposanten en eventuele sprekers met elkaar in contact brengen onder de vorm van een virtueel evenement.

• De virtuele jobbeurs vindt plaats gedurende een overeengekomen periode .

• Alle stakeholders (bezoekers, organisatie, sprekers en exposanten) kunnen tijdens een vooraf bepaalde met elkaar in contact treden via chat en eventueel via videochat.

• Exposanten dienen hun virtuele stand tijdig te reserveren. Hierbij dienen enkele persoonsgegevens te worden verzameld ten behoeve van u, waaronder:

- Naam en voornaam
- Telefoonnummer
- E-mailadres

Doel van het verzamelen van deze persoonsgegevens is de mogelijkheid te bieden aan u om de contactpersoon bij de exposant - die een stand reserveert – te contacteren in het kader van het uitvoeren van een overeenkomst.

• Bezoekers dienen voorafgaand aan het virtueel evenement te registreren via een landingspagina. Hierbij dienen enkele persoonsgegevens te worden verzameld ten behoeve van u, waaronder:

- Naam en voornaam
- E-mailadres

Indien andere, bijkomende persoonsgegevens worden verzameld, dan zullen deze deel uitmaken en automatisch worden toegevoegd van en aan bovenvermelde persoonsgegevens, zonder dat hiervoor een separate bijlage dient opgemaakt en ondertekend te worden.

2. Categorieën van persoonsgegevens

De categorieën van persoonsgegevens die de Verwerkingsverantwoordelijke laat verwerken door ons betreffenden identificatiegegevens. Indien andere, bijkomende persoonsgegevens c.q. categorieën worden verzameld, dan zullen deze deel uitmaken en automatisch worden toegevoegd van en aan bovenvermelde persoonsgegevens c.q. categorieën, zonder dat hiervoor een separate bijlage dient opgemaakt en ondertekend te worden.

3. Categorieën van betrokkenen

De categorieën van betrokkenen van wie de persoonsgegevens verwerkt worden:

- Bezoekers van het virtueel evenement
- Exposanten van het virtueel evenement
- Gegevens van u

4. De verwerking van de persoonsgegevens:

U geeft hierbij de volgende instructies tot verwerking van de persoonsgegevens :

- Persoonsgegevens opslag

Het gaat om diensten van ons waarbij de persoonsgegevens van u opgeslagen worden in een door ons geleverd opslagsysteem zoals onder meer maar niet beperkt tot cloud storage diensten, cloud backup diensten, file diensten, directory diensten, managed file transfer, mail & calendaring and logfile processing.

5. Doorgifte van persoonsgegevens buiten de EER door ons:

- Geen

6. De bewaartermijnen van de persoonsgegevens

Wij bewaren de verwerkte persoonsgegevens op adequaat beveiligde wijze gedurende de periode die nodig is voor het uitvoeren van uw schriftelijke instructies, zijnde 1 maand na het beëindigen van de verwerkingsopdracht.

7. De contactgegevens van de Data Protection Officer (DPO)

- Voor ons:

  Naam: Mike Thevissen (White Wire)

  Contactgegevens (telefoon/GSM): 0472/75 66 22

  Contactgegevens (e-mail): mike.thevissen@whitewire.be

- Voor u:

  Door te sturen naar ons (indien van toepassing)

BIJLAGE 2: PASSENDE TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

De organisatie volgt de wetgeving en rechtspraak inzake de AVG op regelmatige tijdstippen op.

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	