

ALGEMENE VERWERKINGSVOORWAARDEN

versie 1.0 dd. 15/02/2022

Deze Algemene Verwerkingsvoorwaarden vormen de Verwerkingsovereenkomst voor de samenwerking in het kader van de samenwerking in het kader van UiTPAS

TUSSEN

publiq vzw, “Verwerkingsverantwoordelijke”;

EN

de KSB, zoals bedoeld in de basisovereenkomst tussen publiq vzw en KSB, “Verwerker”;

de bovenlokale partner, zoals bedoeld in de samenwerkingsovereenkomst tussen publiq vzw en de bovenlokale partner, “Verwerker”;

en de eventorganisatoren en andere partners waarmee KSB lokaal / regionaal samenwerkt, “Subverwerker”

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

ALGEMENE BEPALINGEN

- A. Deze Algemene Verwerkingsvoorwaarden vormen, samen met de Algemene Voorwaarden, een bijlage bij de Basisoverkomst tussen publiq vzw en KSB enerzijds en tussen KSB en eventorganisator / ander type partner anderzijds, hierna genoemd de Opdracht;
- B. In het kader van UiTPAS zal de Verwerker/Subverwerker bepaalde Persoonsgegevens Verwerken in opdracht en voor rekening van de Verwerkingsverantwoordelijke;

Deze Algemene Verwerkingsvoorwaarden vormen de Verwerkingsovereenkomst en formaliseert de afspraken met betrekking tot de uitvoering en organisatie van deze Verwerking van Persoonsgegevens en maken integraal deel uit van de overeenkomst welke partijen onderling hebben gesloten.

Artikel 1: Definities

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

AVG	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming);
Algemene Verwerkingsvoorwaarden	Dit document en de hierin vervatte bepalingen, welke de afspraken tussen partijen vastlegt inzake de uitvoering en organisatie van de Verwerking van Persoonsgegevens;
Betrokkene	De geïdentificeerde of identificeerbare natuurlijke persoon op wie een Persoonsgegeven betrekking heeft;
Datalek	Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;
Derden	Elke natuurlijke persoon, rechtspersoon, overheidsinstantie, dienst of ander orgaan andere dan de Verwerker, de Verwerkingsverantwoordelijke en hun personeelsleden of aangestelden;
Opdracht	De opdracht zoals omschreven in de (basis)overeenkomst afgesloten tussen partijen;
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals ook gedefinieerd in artikel 4, 1) AVG, die de Verwerker in het kader van de Opdracht Verwerkt;

Unierechtelijke of lidstaatrechtelijke bepaling	Een bepaling opgelegd door Unierechtelijke of (EU) lidstaatrechtelijke wetgeving;
Verwerken / Verwerking	Elke bewerking of geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens, zoals ook gedefinieerd in artikel 4, 2) AVG;
Verwerkingsovereenkomst	Deze Algemene Verwerkingsvoorwaarden.

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

- 2.1. De Verwerker / Subverwerker Verwerkt Persoonsgegevens voor de Verwerkingsverantwoordelijke uitsluitend zoals omschreven in de Opdracht en overeenkomstig de in deze Overeenkomst vastgelegde verplichtingen. De verwerkte Persoonsgegevens worden nader omschreven in bijlage 1.
- 2.2. Elke Verwerking anders dan omschreven in de Opdracht is strikt verboden, met inbegrip van de doorgifte van Persoonsgegevens aan Derden, een derde land of een internationale organisatie, behoudens indien één van de hieronder opgesomde voorwaarden vervuld is:
- de Verwerkingsverantwoordelijke heeft schriftelijke instructies gegeven om bijkomende Verwerkingen uit te voeren; of
 - een Unierechtelijke of lidstaatrechtelijke bepaling verplicht de Verwerker / Subverwerker tot deze bijkomende Verwerking. De Verwerker / Subverwerker zal de Verwerkingsverantwoordelijke desgevallend binnen een redelijke termijn voorafgaand aan de bijkomende Verwerking op de hoogte stellen van voornoemd wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Als de Verwerker / Subverwerker een verzoek krijgt om Persoonsgegevens ter beschikking te stellen door een daartoe bevoegde instantie overeenkomstig een Unierechtelijke of lidstaatrechtelijke bepaling, beoordeelt zij eerst of het verzoek bindend is en of zij op grond van gedrags- en beroepsregels aan het verzoek moet voldoen. Als er geen strafrechtelijke of andere juridische belemmeringen zijn, dan stelt de Verwerker / Subverwerker de Verwerkingsverantwoordelijke op de hoogte van het verzoek. De Verwerker / Subverwerker doet dat binnen een termijn dat het voor de Verwerkingsverantwoordelijke mogelijk is om eventuele rechtsmiddelen tegen de verstrekking van de Persoonsgegevens in te stellen.

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

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

- 3.1. Loopt samen met de Opdracht zoals beschreven in de hoofdovereenkomst welke partijen afsloten met elkaar.
- 3.2. Artikels 3.3, 5, 6, 7, 9 en 12 blijven van kracht na beëindiging van de Verwerkingsovereenkomst.
- 3.3. Na beëindiging van de Verwerkingsovereenkomst dient de Verwerker / Subverwerker aan de Verwerkingsverantwoordelijke zonder onredelijke vertraging, en onverwijld op verzoek, een kopie te bezorgen van alle Persoonsgegevens die door haar in het kader van de Opdracht Verwerkt worden, in gestructureerd, gangbaar en machine leesbaar formaat. Als alle Persoonsgegevens zijn bezorgd, stelt de Verwerker / Subverwerker onmiddellijk een einde aan elke verwerking van de Persoonsgegevens en vernietigt hij elke kopie en back-up van de Persoonsgegevens die hij nog zou bezitten, tenzij opslag van de Persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht.

Artikel 4: Beveiliging (art. 32 AVG)

- 4.1. De Verwerker / Subverwerker treft alle passende technische en organisatorische beveiligingsmaatregelen die nodig zijn om de Persoonsgegevens te beveiligen, rekening houdend met de stand van de techniek en de kost voor beveiliging, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen. In het bijzonder zal de Verwerker / Subverwerker de Persoonsgegevens beveiligen tegen vernietiging, verlies, vervalsing, niet toegelaten verspreiding of toegang en elke andere vorm van onwettige Verwerking. De minimale maatregelen die moeten worden getroffen, worden in bijlage 2 beschreven.
- 4.2. De Verwerker / Subverwerker wijst een functionaris voor gegevensbescherming aan en heeft ten minste een actueel veiligheidsbeleid en -plan.

Artikel 5: Vertrouwelijkheid (art. 29 AVG)

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

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

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

- 6.1. De Verwerker stelt enkel andere verwerkers aan om Persoonsgegevens in het kader van de Opdracht te Verwerken (hierna: de “Subverwerker”) na uitdrukkelijke, specifieke goedkeuring van de Verwerkingsverantwoordelijke. De Verwerkingsverantwoordelijke gaat akkoord met de eventorganisatoren waarmee Verwerker (als KSB) de standaardovereenkomst KSB-eventorganisator afsluit. Voor alle overige subverwerkers blijft uitdrukkelijke en specifieke goedkeuring door Verwerkingsverantwoordelijke (publiq vzw) vereist.
- 6.2. Extern ingehuurde medewerkers worden voor deze Verwerkingsovereenkomst niet als Subverwerker beschouwd. De Verwerker / Subverwerker zal erop toezien dat deze extern ingehuurde medewerkers dezelfde vertrouwelijkheidsclausule, zoals beschreven in artikel 5 van deze Verwerkingsovereenkomst naleven zoals dit voor de eigen werknemers van de Verwerker / Subverwerker het geval is.
- 6.3. De Verwerker en de Subverwerker sluiten een overeenkomst waarin dezelfde verplichtingen inzake gegevensbescherming opgelegd worden als die welke in de voorliggende Verwerkingsovereenkomst zijn opgenomen. De Verwerker zal de Subverwerkers ook dezelfde geheimhoudingsverplichting als deze die op haar rust opleggen middels een vertrouwelijkheidsovereenkomst. De Verwerker / Subverwerker zal op eenvoudig verzoek van de Verwerkingsverantwoordelijke het nodige bewijs voorleggen om aan te tonen dat de overeenkomsten met haar Subverwerkers voldoen aan de in dit artikel gestelde voorwaarden.
- 6.4. De Verwerker / Subverwerker houdt een actueel overzicht bij van de overeenkomsten met Subverwerkers en kan deze binnen redelijke termijn op eenvoudig verzoek bezorgen aan de Verwerkingsverantwoordelijke.
- 6.5. Indien een Subverwerker haar gegevensbeschermingsverplichtingen niet vervult, zal de Verwerker volledig aansprakelijk blijven ten opzichte van de Verwerkingsverantwoordelijke voor de naleving van deze verplichtingen.

Artikel 7: Bijstand (art. 28, lid 3, e - f)

- 7.1. Algemeen

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

7.2. Bijstand bij verzoek van een Betrokkene

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

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

7.3. Bijstand bij Datalekken

De Verwerker / Subverwerker verbindt zich ertoe elk Datalek en alle ernstige pogingen tot onrechtmatige of ongeautoriseerde Verwerkingen of toegangen tot Persoonsgegevens zonder onredelijke vertraging, en uiterlijk 24 uur na kennisname, te melden aan de Verwerkingsverantwoordelijke conform artikel 33.3 van de AVG. De Verwerker / Subverwerker zal alle maatregelen treffen die redelijkerwijs nodig zijn om (verdere) schending van de beveiligingsmaatregelen en eventuele schade te voorkomen of te beperken en zal aan de Verwerkingsverantwoordelijke alle informatie die ze nuttig of nodig acht, verschaffen.

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

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

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

7.4. Andere bijstandsverplichtingen

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

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

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

De Verwerker / Subverwerker Verwerkt de Persoonsgegevens alleen binnen de Europese Economische Ruimte, tenzij hierover met de Verwerkingsverantwoordelijke andere afspraken zijn gemaakt. Deze afspraken leggen de Partijen gezamenlijk schriftelijk vast.

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

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

9.2. Op eenvoudig verzoek van de Verwerkingsverantwoordelijke is de Verwerker / Subverwerker ertoe gehouden alle inlichtingen die van toepassing zijn bij de uitvoering van deze Verwerkingsovereenkomst mee te delen en bijstand te verlenen bij het uitvoeren van de audits of bij het vervullen van de verplichting om verzoeken om uitoefening van de in de AVG vastgestelde rechten van de Betrokkene te beantwoorden.

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

10.1. De Verwerker / Subverwerker is aansprakelijk ten aanzien van de Verwerkingsverantwoordelijke voor schade die voortvloeit uit een handeling of een nalatigheid wanneer bij de Verwerking niet is voldaan aan de specifiek tot Verwerker / Subverwerkers gerichte verplichtingen van de AVG, dan wel uit een handeling of nalatigheid in strijd met de rechtmatige instructies van de Verwerkingsverantwoordelijke.

10.2. De aansprakelijkheid van de Verwerker / Subverwerker is beperkt zoals voorzien in de Opdracht, zonder evenwel afbreuk te doen aan art 82 van de AVG.

Artikel 11: Beëindiging

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

Artikel 12: Overige

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

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

12.3. Aanvullingen en wijzigingen op deze Verwerkingsovereenkomst dienen schriftelijk te gebeuren door middel van een addendum dat als bijlage aan deze Verwerkingsovereenkomst zal worden gehecht. Niettegenstaande de bepalingen van de Basisovereenkomst, staat Het staat publiek vzw als Verwerkingsverantwoordelijke vrij aanvullingen of wijzigingen aan te brengen aan deze Algemene Verwerkingsvoorwaarden, bijvoorbeeld om het gebruik van UTPASdiensten voor alle betrokkenen in de keten mogelijk te maken of te houden.

Dergelijke wijzigingen worden op voorhand meegedeeld aan de Verwerker (KSB), en treden in werking dertig (30) kalenderdagen nadat de wijziging is meegedeeld.

BIJLAGEN

- Bijlage 1: Beschrijving van de Persoonsgegevens
- Bijlage 2: Minimale veiligheidsmaatregelen

BIJLAGE 1

UiTPAS verwerkt de identificatie- en contactgegevens van de houders van een UiTPAS, deelname aan activiteiten en gebruik van de voordelen van UiTPAS, eventueel kansenstatuut en communicatievoorkeuren.

In het kader van Verwerkingsovereenkomst voert de Verwerker op de onderstaande Persoonsgegevens de Verwerkingen uit waarvan per gegevenssoort de aard van de verwerking, alsmede het doel ervan en de categorieën van betrokkenen, de classificatie(*) worden vermeld.

Soort persoonsgegevens	Aard van de verwerking	Doel van de verwerking	Categorie(ën) van betrokkenen	Classificatie (*)
Identificatie en contactgegevens	Persoonlijke identificatiegegevens waaronder naam, voornaam, adres, rijksregisternummer en communicatiekanalen	registratie en identificatie van de pashouder	alle pashouders, al dan niet met kansenstatuut	
Gebruik van het programma	registratie van kaartstelsysteem, eventuele school en deelname aan activiteiten	gebruik en voordelen van het programma	alle pashouders	
Eventueel kansenstatuut	bijzonder statuut, standaard voor personen met recht op verhoogde tegemoetkoming en geldigheidsduur van het statuut	toekennen van kortingtarieven en bijzondere voordelen aan pashouders met kansenstatuut	pashouders met een kansenstatuut	

	in afstemming met KSB kan gebruik worden gemaakt van de koppeling met het MAGDA-platform met het oog op automatische check en/of verlenging van het kansenstatuut (KSZ, automatisch advies)			
Communicatievoorkeuren	opt-in en voorkeuren voor type communicatie	communicatie op maat	alle pashouders	

(*) optioneel

BIJLAGE 2

Technische en Organisatorische maatregelen

Bepalingen art 32 AVG

Rekening houdend 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, treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen.

De verwerker is eraan gehouden om maatregelen te treffen die onder meer het volgende kunnen omvatten:

- de pseudonimisering en versleuteling van persoonsgegevens
- het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen
- het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen
- 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

Technische en organisatorische maatregelen betreffende de interne werking en organisatie.

ALGEMEEN BEVEILIGINGSBELEID EN ORGANISATIE VAN INFORMATIEBEVEILIGING

- **Verantwoordelijke informatiebeveiliging:** Wouter Simons, systeembeheerder, wouter@publiq.be, hierin ondersteund door het platformteam en opsteam van publiq vzw
- **Verantwoordelijke gegevensbescherming:** Davy De Laeter, DPO, davy@publiq.be
- Pashouders kunnen steeds hun vragen stellen via privacy@uitpas.be welke actief worden opgevolgd door helpdeskmedewerkers en waar nodig DPO, dit aan de hand van uitgewerkte en gedocumenteerde procedures en processen.
- **Verantwoordelijkheden op vlak van informatiebeveiliging en gegevensbescherming:** De verantwoordelijkheden van de medewerkers van publiq zijn formeel gedocumenteerd en gepubliceerd in een privacy- en security policy. Elk van de medewerkers ondertekent tevens een verklaring op eer m.b.t. de verwerking van persoonsgegevens en welke als addendum bij de arbeidsovereenkomst wordt gevoegd.
- **Risico analyse, beheer en controle:** publiq vzw voert periodiek risicoanalyses uit van de genomen beveiligingsmaatregelen en doet controles voor wat betreft de naleving van de verschillende informatiebeveiligingsprocedures.

PERSONEEL - VEILIG PERSONEELSBELEID

- **Training over belang van beveiliging en omgang met persoonsgegevens:** publiek vzw voorziet opleidingen om alle medewerkers te sensibiliseren voor wat betreft de beveiligingsrichtlijnen- en beveiligingsprocedures en hun rol daarbij.
- **Toegangsautorisatie:** publiek vzw implementeert en handhaaft een autorisatiebeheersysteem dat de toegang controleert tot systemen die persoonsgegevens bevatten.
Er wordt ter beveiliging met strikte toegangsregels gewerkt opgelegd door middel van onder meer IAM Roles en Bastion hosts. Admin toegang wordt beperkt op basis van IP-ranges.
- **Segregatie:** publiek vzw heeft een segregatie ingevoerd om te vermijden dat personen toegang krijgen tot gegevens waarvoor ze geen toegang nodig hebben voor de uitoefening van hun taak.

GEBOUW

- **Fysieke toegang tot de ruimtes:** publiek vzw beperkt de toegang tot haar ruimtes waar persoonsgegevens verwerkt worden in kader van haar opdracht, strikt tot geïdentificeerde en geautoriseerde personen. Hiertoe werden onder meer badgelezers geïnstalleerd, deuren van sloten voorzien en is er toegangscontrole aan de ingang (medewerker onthaal + registratie bezoekers).
- **Beveiliging van de omgeving:** Naast badgelezers is het volledige gebouw uitgerust met camerabewaking en een alarm- en branddetectiesysteem en inbraakbeveiliging.
- **Firewall:** publiek vzw is uitgerust met een geavanceerde firewall en controlemechanismen die zijn interne netwerk op gepaste wijze beschermt tegen ongeoorloofde toegang tot zijn interne netwerk.

DATACENTER

- **Fysieke toegang tot het datacenter:** publiek vzw centraliseerde alle data die nodig is in kader van haar opdracht in een beveiligd data center conform de industriestandaarden. Fysieke toegang tot het datacenter wordt gecontroleerd en is niet mogelijk voor eigen medewerkers en deze van dienstverleners van publiek vzw.
- **Noodherstel:** publiek vzw beschikt over een noodherstelplan in geval van calamiteiten met haar servers in het datacenter waarop persoonsgegevens staan.
- **Redundantie:** publiek vzw hanteert een back-up beleid dat de nodige redundantie verzekert en gegevensherstel mogelijk maakt.
RDS (Database): 15 dagen backup retentie tot op de seconde herstelbaar / EC2 (Server): Daily (8 back-ups) worden 8 dagen bijgehouden - Weekly (4 stuks) worden 31 dagen bijgehouden - Monthly (6 stuks) worden 181 dagen bijgehouden.

DATA

- **Versleuteling van gegevens:** alle digitale gegevens die verwerkt worden door publiek vzw in kader van haar opdracht worden centraal in het datacenter op een versleutelde manier bewaard op de harde schijven.

Met AWS is een DPA afgesloten specifiek ook in het licht van Schrems II.

Toestellen en disk van medewerkers zijn beveiligd en geëncrypteerd.

De data zijn niet rechtstreeks benaderbaar via het internet, maar enkel via tussenliggende applicaties.

Van de kaarten zelf (RFID/NFC) kan louter het chipnummer worden uitgelezen. Verdere identificatie van de pashouder kan enkel mits login tot een van de toepassingen met voldoende rechten.

- **Anti-virus en beveiligingsupdates:** publiek vzw voorziet al zijn systemen van de laatste updates. Beveiligingsupdates worden opgevolgd en geïnstalleerd volgens het patch management proces.
- **Kwaadaardige software:** publiek vzw voert anti-malwarecontroles uit om te helpen voorkomen dat kwaadaardige software ongeautoriseerde toegang tot klantgegevens krijgt.
- **Logging van toegangen:** publiek vzw voorziet een continue logging op de server van alle toegangen tot haar systemen die persoonsgegevens bevatten met inbegrip van welke gebruiker, de tijd en activiteit. Alle logbestanden worden gedurende 2 jaar bijgehouden.
worden gelogd: gebruiker, IP-adres, tijdsinformatie, gebruikte omgeving, acties en in het bijzonder eventuele export van data indien de gebruiker daar rechten toe heeft - op elk van de toepassingen

COMMUNICATIE

- **Versleuteling van verbindingen:** publiek vzw maakt gebruik van beveiligde verbindingen voor de toegang tot haar gegevens in het datacenter. Alle data die verzonden wordt over publieke netwerken gebeurt dan ook aan de hand van encryptie mechanismen zoals https en waar mogelijk / opportuun VPN.
- **Two-factor authenticatie:** publiek vzw maakt gebruik van een combinatie van gebruikers/wachtwoord en een dynamisch token via sms. Wachtwoorden dienen steeds aan minimale voorwaarden (lengte, samenstelling types karakters, ...) te voldoen.

INFORMATIESYSTEMEN

- **Controle over systeemupdates en evoluties:** publiek vzw heeft een formeel wijzigingsbeheerproces geïmplementeerd om ervoor te zorgen dat wijzigingen in operationele systemen en toepassingen plaatsvinden op een gecontroleerde wijze.
- **Beveiligingsvereisten:** De vereisten voor de bescherming van gegevens en systemen worden geanalyseerd en gespecificeerd in samenwerking met IT-leveranciers.
- **Incident response:** publiek vzw houdt een register van beveiligingsinbreuken bij met een beschrijving van de inbreuk, het tijdstip, de gevolgen van de inbreuk, de naam van de melder en van degene aan wie de inbreuk werd gemeld. Er is een uitgewerkte procedure inzake incident response en bijhorende interne en externe communicatie.
- **Notificatie van incidenten:** In geval van een gegevensbeveiligingsincident dat impact heeft op de vertrouwelijkheid of integriteit van persoonsgegevens van gebruikers, zal publiek vzw, zonder onredelijke vertraging, de verwerkingsverantwoordelijke hiervan informeren.

Van elke verwerker en subverwerker worden minimaal gelijkwaardige maatregelen verwacht.

In het bijzonder zullen verwerkers en subverwerkers:

- waarborgen dat de personen die gemachtigd zijn tot het verwerken van de persoonsgegevens zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen of door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden, onder andere door ondertekening van de "verklaring op eer"
- de passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen, rekening houdend met in het bijzonder de verwerkingsrisico's als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, en te verzekeren dat iedere natuurlijke persoon die handelt onder het gezag van de KSB en toegang heeft tot persoonsgegevens, deze slechts in opdracht van publiek verwerkt, tenzij hij of zij daartoe door het Unierecht of nationaal recht is gehouden.