

Verwerkersovereenkomst

3 September 2026

Deze overeenkomst wordt gesloten tussen:

Gemeente Kortenaken met maatschappelijke zetel gelegen te Dorpsplein 35, 3470 Kortenaken en met ondernemingsnummer BE0207520711, hierbij rechtsgeldig vertegenwoordigd door Kristof Mollu, burgemeester, en Dominique Hayen, algemeen directeur, met functionaris voor gegevensbescherming te bereiken via informatieveiligheid@interleuven.be

hierna: de “Verwerkingsverantwoordelijke”;

en

Vanden Broele NV met maatschappelijke zetel gelegen te Lieven Bauwensstraat 35, 8200 Brugge en met ondernemingsnummer BE0451355351, hierbij rechtsgeldig vertegenwoordigd door Bram Van Impe, General Manager, met Data Protection Officer te bereiken via dpo@vandenbroele.be

hierna: “de Verwerker”;

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

Na te hebben uiteengezet:

De Partijen hebben een overeenkomst of meerdere overeenkomsten (opgesomd in bijlage 1) gesloten met betrekking tot het ontwikkelen, hosten en beheren van één of meerdere softwareproducten van Vanden Broele, hierna genoemd de “Opdracht”;

In het kader van deze overeenkomst zal de Verwerker ook bepaalde Persoonsgegevens Verwerken in opdracht en voor rekening van de Verwerkingsverantwoordelijke. De Opdracht omvat ofwel:

- het leveren van toegang tot een product, website of andere waarbij de Verwerker alle controle over het platform behoudt en de Verwerkingsverantwoordelijke enkel als gebruiker optreedt.
- het uitvoeren van een opdracht waarbij de Verwerker instaat voor het verzamelen, beheer en gebruik van persoonsgegevens.

De partijen wensen nu hun afspraken met betrekking tot de uitvoering en organisatie van deze Verwerking van Persoonsgegevens te formaliseren in deze Verwerkersovereenkomst, die integraal deel uitmaakt van voornoemde dienstverleningsovereenkomst.

De Partijen zijn het volgende overeengekomen:

Artikel 1: Definities

Begrippen die in deze Verwerkersovereenkomst met hoofdletter worden gebruikt, moeten worden geïnterpreteerd zoals in dit artikel of elders in de Verwerkersovereenkomst 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);
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 Betrokkene, de Verwerker, de Subverwerker, de Verwerkingsverantwoordelijke en hun personeelsleden of aangestelden;
Opdracht	De opdracht zoals omschreven in <u>bijlage 1</u> ;
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, zoals ook gedefinieerd in art. 4, lid 1 van de AVG, die de Verwerker in het kader van de Opdracht Verwerkt;
Unierechtelijke of lidstaat-rechtelijke 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 art. 4, lid 2 van de AVG;
Verwerkersovereenkomst	Deze overeenkomst.

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

2.1. De Verwerker Verwerkt Persoonsgegevens voor de Verwerkingsverantwoordelijke uitsluitend zoals omschreven in de Opdracht en overeenkomstig de in deze Overeenkomst vastgelegde verplichtingen. De Opdracht wordt 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 schriftelijk instructies gegeven om bijkomende Verwerkingen uit te voeren; of
- een Unierechtelijke of lidstaatrechtelijke bepaling verplicht de Verwerker tot deze bijkomende Verwerking. De Verwerker 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 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 de Verwerkingsverantwoordelijke op de hoogte van het verzoek. De Verwerker 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 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 van de AVG)

3.1. Deze overeenkomst loopt samen met de Opdracht beschreven in bijlage 1.

3.2. Artikels 5, 6, 7, 9, 10, 11 en 12 blijven van kracht na beëindiging van de Verwerkersovereenkomst.

Artikel 4: Beveiliging (art. 32 van de AVG)

4.1. De Verwerker 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 waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen. In het bijzonder zal de Verwerker de Persoonsgegevens beveiligen tegen vernietiging, verlies, vervalsing, niet toegelaten verspreiding of toegang en elke andere vorm van onwettige Verwerking. De minimale maatregelen die worden getroffen, worden in bijlage 2 toegevoegd.

4.2. De Verwerker wijst een functionaris voor gegevensbescherming aan en heeft tenminste een actueel informatieveiligheidsbeleid- en plan.

Artikel 5: Vertrouwelijkheid (art. 29 van de AVG)

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

5.2. De Verwerker maakt zich sterk dat alle personeelsleden of aangestelden die toegang hebben tot de Persoonsgegevens het vertrouwelijk karakter van deze Persoonsgegevens zullen respecteren. De Verwerker 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 van de AVG)

6.1. Het is de Verwerker toegestaan andere verwerkers aan te stellen om Persoonsgegevens in het kader van de Opdracht te Verwerken (hierna: de "Subverwerker"). De Verwerkingsverantwoordelijke gaat akkoord met de lijst van Subverwerkers opgesomd in bijlage 3. Voor het aannemen van een andere Subverwerker licht de Verwerker de Verwerkingsverantwoordelijke binnen een redelijke termijn in over de toevoeging of verandering. De Verwerkingsverantwoordelijke kan vervolgens bezwaar maken tegen het aannemen van de voorgestelde Subverwerker.

6.2. In geval van bezwaar werken de partijen te goeder trouw samen om een (commercieel) redelijke wijziging door te voeren in de Opdracht waardoor beroep op de voorgestelde Subverwerker vermeden wordt; wanneer deze wijziging niet doorgevoerd kan worden binnen een termijn van 12 maanden na ontvangst van bezwaar door de Verwerker, kan de Verwerkingsverantwoordelijke deze Verwerkersovereenkomst en de overeenkomst of overeenkomsten opgesomd in bijlage 1 met onmiddellijke ingang beëindigen door middel van een schriftelijke kennisgeving aan de Verwerker, voor zover zij betrekking heeft tot de diensten die beroep op de voorgestelde Subverwerker vereisen.

6.3. Extern ingehuurd medewerkers worden voor deze Verwerkersovereenkomst niet als Subverwerker beschouwd. De Verwerker zal erop toezien dat deze extern ingehuurd medewerkers dezelfde vertrouwelijkheidsclausule, zoals beschreven in artikel 5 van deze Verwerkersovereenkomst naleven zoals dit voor de eigen werknemers van de Verwerker het geval is.

6.4. De Verwerker en de Subverwerker sluiten een overeenkomst waarin dezelfde verplichtingen inzake gegevensbescherming opgelegd worden als die welke in de voorliggende Verwerkersovereenkomst zijn opgenomen. De Verwerker zal de Subverwerkers ook dezelfde geheimhoudingsverplichting als deze die op haar rust opleggen middels een vertrouwelijkheidsvereenkomst. De Verwerker 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.

6.5. De Verwerker houdt een actueel overzicht bij van de overeenkomsten met Subverwerkers en kan deze binnen redelijke termijn op eenvoudig verzoek bezorgen aan de Verwerkingsverantwoordelijke.

6.6. 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 van de AVG)

7.1. De Verwerker 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.

De tijd en middelen die de Verwerker spendeert voor het verlenen van de bijstand eigen aan de verantwoordelijkheden van de Verwerker, zijn voor eigen rekening van de Verwerker.

7.2. De Verwerker 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 om zich te beroepen op één van de rechten die hem ingevolge hoofdstuk III van de AVG zijn toegekend, zal de Verwerker dit onverwijld melden aan de Verwerkingsverantwoordelijke en alleen tegemoetkomen aan het verzoek van de Betrokkene na schriftelijk akkoord van de Verwerkingsverantwoordelijke.

7.3. De Verwerker verbindt zich ertoe elk Datalek zonder onredelijke vertraging, en uiterlijk 24 uur na kennisname, te melden aan de Verwerkingsverantwoordelijke conform art. 33 van de AVG. Zelfs bij onvolledige informatie over het Datalek wordt de Verwerkingsverantwoordelijke verwittigd. De Verwerker 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 zij nuttig of nodig acht, verschaffen.

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

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

Het is de Verwerker 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 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 art. 32 van de AVG;
- het uitvoeren van een gegevensbeschermingseffectbeoordeling conform art. 35 van de AVG;
- het voorafgaand aan een voorgenomen verwerking raadplegen van de toezichthoudende autoriteit, wanneer dit na een gegevensbeschermingseffectbeoordeling nodig zou blijken, conform art. 36 van de AVG.

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

8.1. De Verwerker 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 van de AVG)

9.1. De Verwerkingsverantwoordelijke of zijn daartoe aangestelde heeft op elk ogenblik het recht om de naleving van deze Verwerkersovereenkomst te controleren. Daartoe heeft zij het recht om zich ter plaatse te

begeven in de lokalen of plaatsen waar de Verwerker de Verwerking uitvoert. De Verwerkingsverantwoordelijke zal de Verwerker 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 ertoe gehouden alle inlichtingen die van toepassing zijn bij de uitvoering van deze Verwerkersovereenkomst 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.

De Verwerkingsverantwoordelijke kan audits laten uitvoeren door erkende en geaccrediteerde organisaties. De Verwerkingsverantwoordelijke licht hiertoe de Verwerker in over de vooropgestelde scope. De Verwerker kan een audit weigeren indien er al een audit met dezelfde of vergelijkbare scope werd uitgevoerd in de voorbije 12 maanden. De Verwerkingsverantwoordelijke kan in dat geval inzage verkrijgen in de resultaten van die audit.

In audits geconstateerde tekortkomingen worden ter feedback voorgelegd aan de Verwerker voorafgaand aan de oplevering van het finale rapport. De tekortkomingen worden door de Verwerker opgepakt en omgezet tot een plan met corrigerende maatregelen. Dit plan wordt binnen drie maand na vaststelling van de tekortkomingen ter beoordeling en goedkeuring aan Verwerkingsverantwoordelijke aangeboden. De Verwerker draagt voor eigen rekening zorg voor de implementatie van de corrigerende maatregelen en dit in overeenstemming met de timing die in het vooropgestelde plan is opgegeven, tenzij de partijen anders overeenkomen.

9.3. De kosten van de audit zijn ten laste van de Verwerkingsverantwoordelijke.

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

10.1. Artikel 82 van de AVG zet de aansprakelijkheid van Partijen ten aanzien van de Betrokkenen uiteen en bepaalt de eventuele aansprakelijkheidsverdeling en schadevergoedingsregeling tussen de Partijen met betrekking tot de schade berokkend aan de Betrokkenen. Partijen beschouwen de inhoud en verplichtingen van artikel 82 van de AVG als integraal hernomen in de Verwerkersovereenkomst en zullen hier ook volledige uitvoering aan geven.

Artikel 11: Beëindiging (art. 28, lid 3 van de AVG)

11.1. Indien de Verwerker zijn verplichtingen onder deze Verwerkersovereenkomst 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 nalaat passende maatregelen te treffen.

11.2. Wanneer deze Verwerkersovereenkomst eindigt, bezorgt de Verwerker op verzoek van de Verwerkingsverantwoordelijke een actuele kopie van de Persoonsgegevens en van de databank(en) met de Persoonsgegevens die het resultaat zijn van de Verwerking waarmee de Verwerker werd belast in een gestructureerd, gangbaar en machineleesbaar formaat. Deze overdracht gebeurt zonder onredelijke vertraging. De Verwerker bepaalt het formaat en de wijze van de overdracht tenzij de Verwerkingsverantwoordelijke expliciet andere instructies geeft. De Verwerker brengt hiervoor een redelijke kostprijs in rekening in zoals bepaald in de offerte en rekening houdend met effort aan het gangbare dagtarief.

11.3. Als alle Persoonsgegevens en databanken zijn doorgegeven, stelt de Verwerker onmiddellijk een einde aan elke verwerking van de Persoonsgegevens en vernietigt hij elke kopie van de Persoonsgegevens en databanken die hij nog zou bezitten zonder extra kosten voor de Verwerkingsverantwoordelijke, tenzij opslag

van de Persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht. De back-ups worden verwijderd in overeenstemming met het back-upschema van de Verwerker.

11.4. De Verwerker dient na beëindiging van de Opdracht schriftelijk aan de Verwerkingsverantwoordelijke te bevestigen dat artikel 11.3 van deze overeenkomst werd uitgevoerd, en dit binnen een redelijke termijn.

Artikel 12: Overige

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

12.2. Indien een bepaling in de Verwerkersovereenkomst 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 Verwerkersovereenkomst dienen schriftelijk te gebeuren door middel van een addendum dat als bijlage aan deze Verwerkersovereenkomst zal worden gehecht.

Deze Verwerkersovereenkomst werd op 03/09/26 te Brugge opgesteld in evenveel exemplaren als er Partijen zijn. Aan elke Partij wordt één ondertekend exemplaar van de Verwerkersovereenkomst overhandigd.

Voor de Verwerkingsverantwoordelijke,
Elektronisch ondertekend op 4/09/2026
door Kristof Mollu

Kristof Mollu
Burgemeester

Elektronisch ondertekend op 7/09/2026
door Dominique Hayen

Dominique Hayen
Algemeen Directeur

Voor de Verwerker,
 Elektronisch ondertekend op
7/09/2026 door Bram Van Impe,
General Manager

Bram Van Impe
General Manager



BIJLAGEN

- Bijlage 1: Omschrijving Opdracht
- Bijlage 2: Technische en Organisatorische maatregelen
- Bijlage 3: Opsomming van Subverwerkers
- Bijlage 4: Bijvoegsel over deze verwerkersovereenkomst

BIJLAGE 1 – Omschrijving opdracht

Opdracht

De opdracht betreft het ontwikkelen, hosten en beheren van één of meerdere van de softwareproducten van Vanden Broele (niet-exhaustieve lijst). De Verwerkingsverantwoordelijke neemt volgende aangevinkte producten af.

	PRODUCT		DOEL
☒	eGovFlow	1	e-loket voor transactionele dienstverlening
☐	Elexis	2	organisatie bemanning stem- en telbureaus verkiezingen
☐	eSignFlow	3	digitaal ondertekenen documenten
☐	Religiopoint	4	administratie en toezicht eredienstbesturen
☐	Religiosoft	5	boekhouding, interne werking en toezicht eredienstbesturen
☒	ScanSearch (Online)	6	digitaal platform gedigitaliseerde registers en dossiers
☒	Subsidiemanager	7	opzoeken van subsidies en beheer subsidiedossiers
☒	Vanden Broele Account	8	identity provider
☒	Vanden Broele Connect	9	online kennisplatform met informatie per kennisdomein
☒	Vanden Broele Trust Center	10	complianceplatform
☐	Kiezerslijsten en oproepingskaarten	11	indeling verkiezingsbureaus, voorbereiding kiezerslijsten en uitsturen oproepingskaarten

Gegevens

In het kader van Verwerkersovereenkomst voert de Verwerker op de onderstaande Persoonsgegevens de beschreven Verwerkingen uit. De Verwerker past hierbij de principes van rechtmatigheid, behoorlijkheid en transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking en integriteit en vertrouwelijkheid toe. De tabel werd opgemaakt in overeenstemming met het Informatieclassificatieraamwerk van de Vlaamse Overheid (VO-ICR).

KLASSE	SOORT PERSOONSgegevens	PRODUCT	BETROKKENEN
2-00	Professionele contactgegevens: naam, adres, e-mailadres, telefoonnummer, etc.	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	Medewerkers
3-00	Persoonlijke contactgegevens: naam, adres, e-mailadres, telefoonnummer, etc.	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	Medewerkers Burgers
3-01	Identificatiegegevens: IP-adres, cookies, andere unieke identificatoren	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	Medewerkers Burgers
3-02	Persoonlijke kenmerken: nationaliteit, geboortegegevens, geslacht, burgerlijke staat, taal	1, 2, 3, 4, 5, 6, 9, 11	Medewerkers Burgers
3-03	Consumptiegewoonten: logging gebruik toepassing	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11	Medewerkers Burgers
3-04	Woningkenmerken: kadastrale gegevens, EPC, woningtype, etc.	1	Burgers
3-05	Opleiding, ervaring en vorming: gevolgde opleidingen, opleidingsniveau, lidmaatschap beroepsorganisaties, uitgeoefende functies	1, 9	Medewerkers Burgers
3-06	Beroep en betrekking: beroep, relatie tot de werkgever, statuut	1, 2, 3, 4, 5, 7, 9, 11	Medewerkers Burgers
3-08	Rijksregisternummer: rijksregisternummer	1, 2, 3, 4, 5, 11	Medewerkers Burgers
4-00	Financiële en fiscale gegevens: identificatie- en bankrekeningnummers, lasten, inkomsten, uitgaven, subsidies, etc.	1, 4, 5, 7	Burgers
4-01	Leefgewoonten: lidmaatschap vereniging	1	Burgers
4-02	Fysieke kenmerken, medische of psychische gegevens en behandelingen: beperking	1	Burgers
4-03	Samenstelling van het gezin: samenlevingsvormen, relatie met andere rechtstreekse verwanten, aantal kinderen, aantal gezinsleden, etc.	1	Burgers
4-04	Juridische en gerechtelijke gegevens: uittreksels strafregister	1, 4	Burgers
4-07	Politieke, filosofische of religieuze relaties en overtuigingen: lidmaatschap of steun van religieuze organisatie	4, 5	Burgers Medewerkers

BIJLAGE 2 – Technische en Organisatorische maatregelen

Bepalingen (art. 32 van de 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.

ISO 27001-certificatie

Vanden Broele is gecertificeerd op de managementstandaard ISO 27001. Vanden Broele onderhoudt een Information Security Management System (ISMS) waarin het volledige, door het management goedgekeurde, informatieveiligheidsbeleid is opgenomen. De daarmee samenhangende plan-do-check-act-cyclus (PDCA) garandeert dat er systematisch wordt ingezet op het identificeren en mitigeren van risico's. De uitgezette acties vertalen zich in passende technische en organisatorische maatregelen, die in deze bijlage verder worden beschreven. Het certificaat kan worden geraadpleegd op <https://www.vandenbroele.be/nl-be/landing/iso-27001>. Meer informatie hierover kan worden verkregen via de Chief Information Security Officer op ciso@vandenbroele.be en de Data Protection Officer (DPO) op dpo@vandenbroele.be.



Interne werking en organisatie van Vanden Broele

BELEID		
ALGEMEEN BEVEILIGINGSBELEID EN ORGANISATIE VAN INFORMATIEVEILIGHEID	✓	Risico analyse, beheer en controle: Vanden Broele voert periodiek risicoanalyses uit van de genomen beveiligingsmaatregelen en doet controles voor wat betreft de naleving van de verschillende informatiebeveiligingsprocedures.
	✓	Verantwoordelijke voor informatieveiligheid: Vanden Broele heeft een Chief Information Security Officer (CISO) aangesteld die verantwoordelijk is voor informatieveiligheid. De CISO coördineert en onderhoudt managementsysteem voor informatieveiligheid.
	✓	Verantwoordelijke voor gegevensbescherming: Vanden Broele heeft een Data Protection Officer (DPO) aangesteld die verantwoordelijk is voor het coördineren, opvolgen en controleren van de beveiligingsregels en -procedures.
	✓	Verantwoordelijkheden op vlak van informatieveiligheid en gegevensbescherming: De verantwoordelijkheden van de medewerkers van Vanden Broele zijn formeel gedocumenteerd en gepubliceerd.

PERSONEEL		
VEILIG PERSONEELSBELEID	✓	Training over belang van beveiliging en omgang met persoonsgegevens: Vanden Broele voorziet opleidingen om alle medewerkers te sensibiliseren voor wat betreft de beveiligingsrichtlijnen- en beveiligingsprocedures en hun rol daarbij.
	✓	Toegangsautorisatie: Vanden Broele implementeert en handhaaft een autorisatiebeheersysteem dat de toegang controleert tot systemen die persoonsgegevens bevatten.
	✓	

		Segregatie: Vanden Broele 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 BEVEILIGING	✓	Fysieke toegang tot productie- en bureauruimtes: Vanden Broele beperkt de toegang tot haar ruimtes waar persoonsgegevens verwerkt worden in kader van haar opdracht, strikt tot geïdentificeerde en geautoriseerde personen. Hiervoor werden badgelezers geïnstalleerd en werden sloten voorzien op deuren waar nog nodig, dit alles om ongeoorloofde toegang te vermijden.
	✓	Beveiliging van de omgeving: Naast badgelezers is het volledige gebouw uitgerust met camerabewaking en een alarm- en branddetectiesysteem.
BESCHERMING TEGEN ONGEREGLDHEDEN, PANNES EN INCIDENTEN	✓	Firewall: Vanden Broele is uitgerust met een geavanceerde firewall en controlemechanismen die zijn interne netwerk op gepaste wijze beschermt tegen ongeoorloofde toegang.

DATACENTER		
FYSIEKE BEVEILIGING	✓	Fysieke toegang tot het datacenter: Vanden Broele centraliseerde alle data die nodig is in kader van haar opdracht in een beveiligd datacenter conform de industriënormen. Fysieke toegang tot het datacenter wordt gecontroleerd/beheerd.
	✓	Noodherstel: Vanden Broele beschikt over een noodherstelplan in geval van calamiteiten met haar servers in het datacenter waarop persoonsgegevens staan.
	✓	Redundantie: Vanden Broele bewaart kopieën van persoonsgegevens alsook haar gegevensherstelprocedures welke opgeslagen staan in het primaire datacenter in een tweede datacenter.

DATA		
DIGITALE GEGEVENS	✓	Versleuteling van gegevens: Alle digitale gegevens die verwerkt worden door Vanden Broele in het kader van de opdracht worden centraal in het datacenter bewaard en waar gepast op een versleutelde manier bewaard op zowel de fysieke dragers als op de virtuele volumes.
	✓	Antivirus en beveiligingsupdates: Alle systemen zijn voorzien van de laatste updates. Beveiligingsupdates worden opgevolgd en geïnstalleerd volgens haar patchmanagementproces.
	✓	Kwaadaardige software: Vanden Broele voert anti-malwarecontroles uit om te helpen voorkomen dat kwaadaardige software ongeautoriseerde toegang tot klantgegevens krijgt.
	✓	Logging van toegangen: Vanden Broele voorziet een continue logging op de server van alle toegangen tot de systemen met inbegrip van welke gebruiker, de tijd en activiteit. Alle logbestanden worden tenminste gedurende 30 dagen bijgehouden.

COMMUNICATIE		
BEVEILIGDE VERBINDINGEN	✓	Versleuteling van verbindingen: Vanden Broele 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 encryptiemechanismen zoals https en VPN.
AUTHENTICATIE	✓	Tweestapsverificatie, wachtwoorden en accounts: Toegang verloopt geauthenticeerd en wordt verstrekt op individuele basis en bij voorkeur wordt tweestapsverificatie toegepast. Het wachtwoord dient te voldoen aan actuele normen voor een veilig wachtwoord.

INFORMATIESYSTEMEN		
ONDERHOUD EN EVOLUTIE VAN INFORMATIESYSTEMEN	✓	Controle over systeemupdates en evoluties: Er wordt 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 onze IT leverancier(s).
INCIDENTEN	✓	Incident response: Vanden Broele 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.
	✓	Notificatie van incidenten: In geval van een informatieveiligheidsincident dat impact heeft op de vertrouwelijkheid of integriteit van persoonsgegevens van klanten, informeert Vanden Broele zonder onredelijke vertraging de verwerkingsverantwoordelijke.

VTC-vragenlijst

Vragenlijst inzake aanwezigheid en effectiviteit van de Organisatorische en Technische maatregelen voor de bescherming van (persoons)gegevens.

BESCHRIJVING VAN DE DIENST		
Is de documentatie inzake de geleverde dienst actueel en accuraat?	✓	Verwerkingsregister
Werd de verwerkingsverantwoordelijke op de hoogte gebracht van eventuele (recente) wijzigingen aan de geleverde dienst?	✓	
Werd/wordt er een verwerkingsovereenkomst ondertekend voor de verwerking werd aangevat? Werd/wordt deze aangepast voor eventuele wijziging?	✓	Verwerkersovereenkomst

ORGANISATORISCHE MAATREGELEN		
A.5.1 - Is er een duidelijke security policy die alle domeinen van de ISO 27001/27002 afdekt – rekening houdende met beschreven “te beschouwen dimensies”?	✓	Informatieveiligheidsbeleid
A.5.2 - Zijn de rollen en verantwoordelijkheden vastgelegd met name in zake CISO, DPO, operationeel beheer, incidentenbeheer?	✓	Rollen en verantwoordelijkheden
A.5.3 - Is functiescheiding toegepast om ongeoorloofde acties onmogelijk te maken?	✓	Toegangsbeleid
A.5.12/A.5.13 - Wordt er een classificatie van data en van systemen toegepast?	✓	Informatieclassificatiebeleid
A.5.15/A.5.16/A.5.17/A.5.18 - Is er een strikt gebruikers- en toegangsbeheer? Met name voor geprivilegieerde beheerders?	✓	Toegangsbeleid; Autorisatiebeheerproces
A.5.19 - Worden de contractuele verplichtingen 1-op-1 doorgezet naar uw subverwerkers en houdt u daar minimaal jaarlijks toezicht op?	✓	Leveranciersbeleid
A.5.20 - Worden alle belangrijke activiteiten (met name van beheerders) in onwiltbare audittrails vastgelegd die toegankelijk zijn voor de verwerkingsverantwoordelijke?	✓	Logging- en monitoringbeleid
A.5.21/A.5.22/A.5.23 - Hebt u duidelijke regels inzake levering en gebruik van software en hardware en (security) testing – toepasselijk voor elke wijziging? Voorziet u al uw systemen van de laatste updates en worden beveiligingsupdates opgevolgd en geïnstalleerd volgens een patchmanagementproces? Voert u anti-malwarecontroles uit om te helpen voorkomen dat kwaadaardige software ongeautoriseerde toegang tot klantgegevens krijgt?	✓	Leveranciersbeleid; Product software testbeleid
A.5.24/A.5.25/A.5.26/A.5.27/A.5.28 - Zijn er duidelijke systemen en processen voor het beheeren (en coördineren) van veiligheidsincidenten?	✓	Incidentenbeleid
A.5.34 - Kent u de regels inzake privacybescherming en de bescherming van persoonsgegevens en past u die toe? Worden de vereisten voor de bescherming van gegevens en systemen geanalyseerd en gespecificeerd in samenwerking met de IT-leverancier(s) (subverwerkers)? Houdt u 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?	✓	Privacybeleid; Wettelijke en contractuele vereisten

PERSONELE MAATREGELEN		
A.6.1/A.6.2/A.6.3 - Zijn er duidelijke regels en is er toezicht op gedrag van geprivilegieerde beheerders? Worden veiligheidsregels jaarlijks herhaald in hun training?	✓	Toegangsbeleid; Logging- en monitoringbeleid; Rollen en verantwoordelijkheden
A.6.4/A.6.5/A.6.6 - Zijn er duidelijke regels in geval van non-compliant gedrag? Bij het veranderen van functie of verlaten van de firma? Zijn al uw medewerkers gebonden door een geheimhoudingsclausule?	✓	Arbeidsreglement; Arbeidsovereenkomst; Geheimhoudings-overeenkomst
A.6.7/A.6.8 - Zijn er duidelijke regels inzake werken op afstand (enkel middels systemen van de verwerker)? Zijn er duidelijke regels over het rapporteren van eventuele/mogelijke veiligheidsincidenten?	✓	Arbeidsreglement; Telewerkovereenkomst; Acceptable use beleid; Incidentenbeleid

FYSIEKE MAATREGELEN		
---------------------	--	--

A.7.1/A.7.2/A.7.3/A.7.4 - Zijn de toegang tot de systemen en de systemen die gebruikt worden bij beheer op niveau?	✓	Fysiek beveiligingsbeleid
A.7.5/A.7.6/A.7.7/A.7.8/A.7.10/A.7.11 - Zijn adequate maatregelen getroffen die ongeautoriseerde toegang tot systemen en dragers van data in principe onmogelijk maken?	✓	Fysiek beveiligingsbeleid; Beheer fysieke beveiliging; Acceptable use beleid

TECHNOLOGISCHE MAATREGELEN		
A.8.1 - Beschikken beheerders over adequate en beveiligde systemen?	✓	Acceptable use beleid
A.8.2/A.8.3/A.8.4 - Hebt u een aparte privileged access management omgeving (PAM)? Wordt voor (beheers)toegang op afstand gebruik gemaakt van een VPN? En is toegang beperkt tot een need-to-know?	✓	Toegangsbeleid; Autorisatiebeheer-proces
A.8.5 - Past u sterke authenticatie toe op al uw processen en MFA voor alle geprivilegieerde toegangen?	✓	Wachtwoordbeleid
A.8.7/A.8.8 - Zijn uw systemen maximaal beschermd tegen malware? Test u uw systemen adequaat tegen kwetsbaarheden?	✓	Acceptable use beleid; Threat intelligence beleid
A.8.10/A.8.11/A.8.12 - Beschermt u data adequaat en conform hun CIA-classificatieniveaus?	✓	Informatiebeheerbeleid; Acceptable use beleid
A.8.13 - Beschikt u conform de CIA-classificatie over de nodige back-up en disaster recovery systemen?	✓	Back-upbeleid
A.8.15/A.8.16 - Beschikt u over adequate logging en monitoring om security incidenten te kunnen detecteren?	✓	Logging- en monitoringbeleid
A.8.20/A.8.21/A.8.22 - Is de infrastructuur opgezet om data en systemen adequaat genoeg te scheiden?	✓	Pentestbeleid infra
A.8.24 - Past u waar nodig adequate cryptografische maatregelen toe zoals signing of encryptie? Gebruikt u beveiligde verbindingen voor de toegang tot uw gegevens in het datacenter? Gebeurt het verzenden van data over publieke netwerken aan de hand van encryptiemechanismen?	✓	Cryptografiebeleid
A.8.25/A.8.26/A.8.27/A.8.28/A.8.29 - Heeft u een software delivery pipeline die elke code-/config-wijziging valideert op fouten/non-compliances ...?	✓	Beleid voor veilig ontwikkelen (SDLC); Software-ontwikkelings-proces (SDLC-proces)

BIJLAGE 3 – Opsomming van Subverwerkers

NAAM	ADRES	TAAK
Amazon Web Services EMEA SARL	38 Av. John F. Kennedy 1855 Luxembourg Luxemburg	Hostingpartner van data op cloudservers in een datacenter in Ierland, specifiek voor processen in eGovFlow met uitzondering van de burgerzaken-processen (Bevolking, Burgerlijke Stand en Strafrecht) (1)
Datargus	Lieven Bauwensstraat 33 8200 Brugge België 0464.441.245	Scanning i.f.v. ScanSearch en ScanSearch Online (6)
Flowsparks	Ottergemsesteenweg-Zuid 808 bus 545 9000 Gent België 0460.563.918	Integratie e-learnings (9)
INNI group	Industrielaan 5 8501 Heule 0418.420.485 België	Drukwerk verkiezingen (10)
Kinamo NV	Hessenstraatje 2 2000 Antwerpen België 0861.077.215	Hostingpartner van data op dedicated fysieke servers in een datacenter in België (1, 2, 3, 4, 5, 6, 7, 8, 9)
Microsoft Corporation	1 Microsoft Way Redmond, Washington 98052-83000 Verenigde Staten	Ontwikkeling, beveiliging, analytics en CRM via DevOps, Microsoft Azure, Security (Microsoft Defender), Analytics (PowerBI) en Microsoft Dynamics 365 in regio West-Europa (1, 2, 3, 4, 5, 6, 7, 8, 9)
Piwik PRO SA	ul. św. Antoniego 2/4 50-073 Wrocław Polen 0464.411.245	Analytics en consent management van cookies op cloudservers in een datacenter in Nederland (1, 3, 7, 9)