VERWERKERSOVEREENKOMST ZORGPROFESSIONALS

De ondergetekenden:

1. Verloskundigen- of huisartsenpraktijk, ingeschreven in de kamer van koophandel, gevestigd op het adres, de postcode en plaats zoals ingevoerd in het registratieformulier van anticonceptieportaal.nl (hierna te noemen “Verwerkingsverantwoordelijke”);

en

2. J&J Software BV (hierna: “Software BV”), een besloten vennootschap met beperkte aansprakelijkheid, statutair gevestigd te Oegstgeest, kantoorhoudende aan het Wilhelminapark 22, 2342 AH te Oegstgeest, ingeschreven bij de Kamer van Koophandel onder nummer 98576860 (hierna te noemen “Verwerker”).

Gezamenlijk hierna ook te noemen “Partijen”,

In overweging nemende dat:

- Verwerkingsverantwoordelijke een verloskundigen- of huisartsenpraktijk heeft en in dat kader gebruik maakt van de automatiseringsapplicatie van Software BV waarmee medische hulpmiddelen, anticonceptie- en geneesmiddelen elektronisch voorgeschreven en recepten elektronisch verwerkt kunnen worden (hierna: “Dienst”);
- Verwerker in het kader van de Dienst (bijzondere) persoonsgegevens van patiënten van Verwerkingsverantwoordelijke verzamelt en deze met behulp van de applicatie opslaat, verwerkt en ter beschikking stelt van Apotheek Beker C.V., gevestigd aan de Lijtweg 4, 2341 HA te Oegstgeest en Apotheek Haaswijk gevestigd aan het Boerhaveplein 21, 2343 LT te Oegstgeest.
- Verwerker de patiëntgegevens in geanonimiseerde vorm mag gebruiken voor het opstellen van benchmark data per praktijk;
- Verwerkingsverantwoordelijke ten aanzien van de verwerking van persoonsgegevens als verwerkingsverantwoordelijke in de zin van artikel 4 aanhef en onder 7 van de Algemene verordening gegevensbescherming (“AVG”) is aan te merken;
- Verwerker ten aanzien van het voor Verwerkingsverantwoordelijke opslaan en ter beschikking stellen van de persoonsgegevens als verwerker in de zin van artikel 4 aanhef en onder 8 AVG is aan te merken;
- Partijen – mede ter uitvoering van het bepaalde in artikel 28, derde lid, AVG – in de onderhavige overeenkomst een aantal voorwaarden wensen vast te leggen die van toepassing zijn op hun relatie in verband met de (verwerking van persoonsgegevens in het kader van) genoemde activiteiten in opdracht van en ten behoeve van Verwerkingsverantwoordelijke.

Verklaren als volgt te zijn overeengekomen:

Artikel 1 Definities

1.1 In deze Verwerkersovereenkomst hebben de volgende begrippen, steeds met een hoofdletter geschreven, de volgende betekenis ongeacht of deze in meervoud of enkelvoud worden gebruikt:

a. Annex: aanhangsel bij de Verwerkersovereenkomst, dat onlosmakelijk deel uitmaakt van de Verwerkersovereenkomst;

b. Verwerkersovereenkomst: de onderhavige overeenkomst;

c. Gebruiksovereenkomst: de tussen Verwerkingsverantwoordelijke en Verwerker gesloten overeenkomst ten aanzien van het gebruik van de Dienst van de Verwerker door de Verwerkingsverantwoordelijke;

d. Persoonsgegevens: alle informatie die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon, als bedoeld in artikel 4 aanhef en 1 AVG;

e. Verwerken: het verwerken van Persoonsgegevens als bedoeld in artikel 4 aanhef en onder 2 AVG.

1.2 Voor zover begrippen welke met een hoofdletter worden geschreven hierboven niet worden gedefinieerd, is de betreffende definitie in de Gebruiksovereenkomst opgenomen.

Artikel 2 Verwerkingsverantwoordelijke voor en Verwerker van de gegevens

2.1 Verwerkingsverantwoordelijke en Verwerker hebben onderhavige Verwerkersovereenkomst gesloten met betrekking tot uitvoering van de Gebruiksovereenkomst. Verwerker verbindt zich in het kader van deze Verwerkersovereenkomst in opdracht van Verwerkingsverantwoordelijke Persoonsgegevens te Verwerken. Een overzicht van het soort Persoonsgegevens, de categorieën van betrokkenen en doelen waarvoor de Verwerking van Persoonsgegevens plaatsvindt, is opgenomen in Annex 1.

2.2 Verwerkingsverantwoordelijke garandeert dat de opdracht tot Verwerking van die Persoonsgegevens in overeenstemming is met alle toepasselijke wet- en regelgeving. Verwerkingsverantwoordelijke vrijwaart Verwerker tegen alle aanspraken van derden welke op enigerlei wijze voortvloeien uit het niet naleven van deze garantie.

2.3 Verwerker verbindt zich uitsluitend persoonsgegevens te Verwerken ten behoeve van de in deze Verwerkersovereenkomst genoemde activiteiten. Verwerker mag de Persoonsgegevens in geanonimiseerde vorm gebruiken voor benchmark doeleinden. Verwerker garandeert dat zij, zonder uitdrukkelijke en schriftelijke toestemming van Verwerkingsverantwoordelijke, op geen enkele andere wijze gebruik zal maken van de Persoonsgegevens die onder deze Verwerkersovereenkomst en/of Gebruiksovereenkomst worden Verwerkt, tenzij een op de Verwerker van toepassing zijnde wettelijke bepaling hem tot verwerking verplicht. In dat geval stelt de Verwerker de Verwerkingsverantwoordelijke, voorafgaand aan de Verwerking, in kennis van dat wettelijke voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

Artikel 3 Technische en organisatorische maatregelen

3.1 Verwerker zal passende technische en organisatorische maatregelen ten uitvoer (laten) leggen om Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige Verwerking en zo een op het risico afgestemd beveiligingsniveau te waarborgen. Deze maatregelen zullen, rekening houdend met de stand der techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau garanderen, gelet op de risico's die de Verwerking en de aard van de te beschermen gegevens met zich meebrengen. Verwerker zal in ieder geval maatregelen nemen om Persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk hetzij onrechtmatig, tegen toevallig en opzettelijk verlies, vervalsing, niet toegelaten verspreiding of toegang, dan wel tegen enige andere vorm van onrechtmatige Verwerking.

3.2 De door Verwerker genomen technische en organisatorische maatregelen staan beschreven in Annex 2. Verwerkingsverantwoordelijke erkent kennis te hebben genomen van de betreffende maatregelen en door ondertekening van deze Verwerkersovereenkomst gaat Verwerkingsverantwoordelijke akkoord met de door Verwerker genomen maatregelen.

3.3 Verwerker zal Verwerkingsverantwoordelijke, voor zover redelijkerwijs mogelijk, bijstand verlenen bij het doen nakomen van diens verplichting onder de AVG om passende technische en organisatorische maatregelen te treffen om een op het risico afgestemd beveiligingsniveau te waarborgen.

Artikel 4 Vertrouwelijkheid

4.1 Verwerker zal al haar medewerkers, die betrokken zijn bij de uitvoering van de Gebruiksovereenkomst, een geheimhoudingsverklaring – al dan niet opgenomen in de arbeidsovereenkomst met die medewerkers – laten ondertekenen waarin in ieder geval is opgenomen dat deze medewerkers geheimhouding moeten betrachten ten aanzien van de Persoonsgegevens. Verwerker neemt zodanige maatregelen, zoals screening van medewerkers en beveiliging van gegevensdragers, teneinde te garanderen dat deze geheimhoudingsplicht wordt nagekomen.

Artikel 5 Gegevensverwerking buiten Nederland

5.1 Het overbrengen van Persoonsgegevens door Verwerker buiten de Europese Economische Ruimte is alleen toegestaan met inachtneming van de daarvoor geldende wettelijke verplichtingen, waarbij Verwerker Verwerkingsverantwoordelijke vooraf zal informeren van de betreffende doorgifte dan wel zo nodig diens voorafgaande schriftelijke toestemming zal vragen, welke toestemming niet op onredelijke gronden zal worden geweigerd.

Artikel 6 Inschakeling Sub Verwerker

6.1 Het is Verwerker toegestaan om in het kader van deze Verwerkersovereenkomst en de Gebruiksovereenkomst gebruik te maken van onderaannemers ("Sub Verwerkers"), zoals opgenomen in Annex 1. Indien Verwerker een andere Sub Verwerker wenst in te schakelen, zal Verwerker de Verwerkingsverantwoordelijke inlichten over de beoogde veranderingen en de Verwerkingsverantwoordelijke de mogelijkheid bieden om tegen deze veranderingen bezwaar te maken.

6.2 Verwerker verplicht iedere Sub Verwerker contractueel minimaal dezelfde verplichtingen inzake gegevensbescherming op te leggen zoals bepaald in deze Verwerkersovereenkomst, waaronder met name de geheimhoudingsverplichtingen, meldingsverplichtingen en beveiligingsmaatregelen.

Artikel 7 Aansprakelijkheid

7.1 Het bepaalde in de Gebruiksovereenkomst inzake de beperking van aansprakelijkheid is van overeenkomstige toepassing.

7.2 Onverminderd artikel 7.1 van deze Verwerkersovereenkomst, is Verwerker slechts aansprakelijk voor de schade die door Verwerking is veroorzaakt wanneer bij deze Verwerking niet is voldaan aan specifiek tot Verwerker gerichte verplichtingen van de AVG, buiten dan wel in strijd met de rechtmatige instructies van Verwerkingsverantwoordelijke is gehandeld of wanneer Verwerker toerekenbaar tekort is geschoten in de nakoming van de Verwerkersovereenkomst.

Artikel 8 Inbreuk in verband met persoonsgegevens

8.1 Indien Verwerker kennis krijgt van een inbreuk in verband met Persoonsgegevens zoals gedefinieerd in de AVG en/of enig ander incident ten aanzien van de beveiliging van Persoonsgegevens, zal zij i) Verwerkingsverantwoordelijke daarvan binnen twee werkdagen op de hoogte stellen en ii) alle redelijke maatregelen nemen om (verdere) schending van de AVG te voorkomen of te beperken.

8.2 Verwerker zal, voor zover redelijk, haar medewerking verlenen aan Verwerkingsverantwoordelijke en Verwerkingsverantwoordelijke ondersteunen in het uitvoeren van haar wettelijke verplichtingen ten aanzien van het geconstateerde incident. Verwerker zal voor zover redelijk Verwerkingsverantwoordelijke ondersteunen bij de op Verwerkingsverantwoordelijke rustende meldplicht ten aanzien van de inbreuk in verband met persoonsgegevens bij de Autoriteit Persoonsgegevens en/of de betrokkene, zoals bedoeld in artikelen 33, lid 3, en 34, lid 1, AVG. Verwerker is nimmer gehouden tot het melden van een inbreuk in verband met Persoonsgegevens bij de Autoriteit Persoonsgegevens en/of de betrokkene.

8.3 Verwerker is nimmer aansprakelijk voor de (correcte en/of tijdige uitvoering van de) op Verwerkingsverantwoordelijke rustende meldplicht zoals bedoeld in artikelen 33 en 34 AVG.

8.4 De Verwerker documenteert alle inbreuken in verband met Persoonsgegevens als bedoeld in artikel 8.1 van deze Verwerkersovereenkomst, met inbegrip van de feiten omtrent de inbreuk in verband met Persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Deze documentatie verstrekt de Verwerker uitsluitend aan de Verwerkingsverantwoordelijke in geval van een verzoek van de toezichthoudende autoriteit aan de Verwerkingsverantwoordelijke, als bedoeld in artikel 33 lid 5 AVG.

Artikel 9 Bijstand aan Verwerkingsverantwoordelijke

9.1 Verwerker zal Verwerkingsverantwoordelijke, voor zover redelijkerwijs mogelijk, bijstand verlenen bij het vervullen van diens plicht onder de AVG om verzoeken om uitoefening van de rechten van een betrokkene te beantwoorden, in het bijzonder het recht op inzage (art. 15 AVG), rectificatie (art. 16 AVG), gegevenswissing (art. 17 AVG), beperking (art. 18 AVG), overdraagbaarheid (art. 20 AVG) en het recht van bezwaar (art. 21 en 22 AVG). Verwerker zal een klacht of een verzoek van een betrokkene met betrekking tot de Verwerking van Persoonsgegevens binnen vijf (5) werkdagen doorsturen naar de Verwerkingsverantwoordelijke, die verantwoordelijk is voor de afhandeling van het verzoek. Verwerker is gerechtigd de eventuele kosten die gemoeid zijn met de medewerking, in rekening te brengen bij Verwerkingsverantwoordelijke.

9.2 Verwerker zal Verwerkingsverantwoordelijke, voor zover redelijkerwijs mogelijk, bijstand verlenen bij het doen nakomen van diens plicht onder de AVG om een gegevensbeschermingseffectbeoordeling

(art. 35 en 36 AVG) uit te voeren. Verwerker is gerechtigd de eventuele kosten die hiermee gemoeid zijn, in rekening te brengen bij de Verwerkingsverantwoordelijke.

9.3 Verwerker zal de Verwerkingsverantwoordelijke alle informatie ter beschikking stellen die nodig is om aan te tonen dat Verwerker voldoet aan haar verplichtingen onder de AVG. Voorts zal Verwerker op verzoek van Verwerkingsverantwoordelijke audits, waaronder inspecties, door Verwerkingsverantwoordelijke of een door Verwerkingsverantwoordelijke gemachtigde controleur mogelijk maken en eraan bijdragen. Verwerker is gerechtigd de eventuele kosten die hiermee gemoeid zijn, in rekening te brengen bij Verwerkingsverantwoordelijke, tenzij uit een dergelijke controle blijkt dat sprake is van aantoonbaar ernstige verwijtbare nalatigheid aan de zijde van Verwerker met betrekking tot het doorvoeren van de in Annex 2 van de Verwerkersovereenkomst overeengekomen beveiligingsmaatregelen.

Artikel 10 Beëindiging & Varia

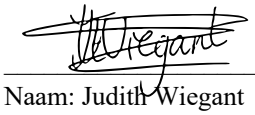
10.1 De Verwerkersovereenkomst eindigt op het moment dat de Gebruiksovereenkomst eindigt, tenzij na beëindiging van de Gebruiksovereenkomst, om wat voor reden dan ook, Verwerker nog steeds Persoonsgegevens Verwerkt of onder zich heeft, in welk geval de Verwerkersovereenkomst van toepassing is zolang Verwerker Persoonsgegevens Verwerkt. Onverminderd de specifieke bepalingen uit de Gebruiksovereenkomst, zal de Verwerker op eerste verzoek van de Verwerkingsverantwoordelijke alle Persoonsgegevens wissen of deze aan hem terugbezorgen, en bestaande kopieën verwijderen, tenzij Verwerker wettelijk verplicht is de Persoonsgegevens op te slaan. Verwerker zal Verwerkingsverantwoordelijke een schriftelijke bevestiging sturen zodra de Persoonsgegevens op verzoek van Verwerkingsverantwoordelijke zijn vernietigd.

10.2 Verwerkingsverantwoordelijke zal Verwerker adequaat informeren over (wettelijke) bewaartermijnen die van toepassing zijn op de Verwerking van Persoonsgegevens voor Verwerker. Verwerker zal de Persoonsgegevens niet langer Verwerken dan overeenkomstig deze bewaartermijnen.

10.3 De verplichtingen uit deze Verwerkersovereenkomst die naar hun aard bestemd zijn om beëindiging te overleven, blijven ook na beëindiging van deze Verwerkersovereenkomst van kracht.

Aldus overeengekomen en ondertekend door Verwerker en elektronisch geaccepteerd door Verwerkingsverantwoordelijke,

Namens Verwerker



Naam: Judith Wiegant
Functie: Directeur
Plaats: Oegstgeest
Datum: 9 oktober 2026

Annex 1

Dienst van Verwerker:

Verwerker stelt aan Verwerkingsverantwoordelijke een automatiseringsapplicatie beschikbaar waarmee medische hulpmiddelen, anticonceptie- en geneesmiddelen elektronisch voorgeschreven kunnen worden door zorgprofessionals (o.a. verloskundigen en huisartsen) en recepten door Apotheek Beker of Apotheek Haaswijk verwerkt kunnen worden, de patiënt het medisch hulpmiddel, anticonceptie- of geneesmiddel online kan afrekenen, een digitale factuur van Apotheek Beker of Apotheek Haaswijk ontvangt en het medisch hulpmiddel, anticonceptie- of geneesmiddel bij de verloskundigen- of huisartsenpraktijk bezorgd wordt.

Deze dienst die door Verwerker wordt geleverd is beschreven in de Gebruiksovereenkomst.

De Persoonsgegevens zijn uitsluitend beschikbaar in digitale vorm.

De verwerking vindt plaats voor de volgende doelen:

Om de online totaaloplossing te bieden, bestaande uit:

- Voorschrijven van medisch hulpmiddel, anticonceptie- of geneesmiddel door zorgprofessionals (o.a. verloskundigen- en huisartsenpraktijken)
- Ter hand stellen van geneesmiddelen door apotheker;
- Online betaling door patiënt aan apotheker;
- Versturen van online factuur door apotheker aan patiënt.

De verwerking vindt ook plaats om de softwaresystemen te implementeren en onderhouden.

De verwerking heeft betrekking op de volgende categorieën van betrokkenen:

- Contactgegevens per verwerkingsverantwoordelijke (“Zorgprofessional gegevens”);
- Gegevens die Verwerkingsverantwoordelijke verstrekt aan Verwerker voor de verwerkingsdoeleinden (“Patiënt- en receptgegevens”);

Verwerker zal de volgende soort Persoonsgegevens verwerken:

Zorgprofessional gegevens:

- Naam praktijk
- Adres
- Postcode
- Plaats
- Voornaam zorgprofessional
- Achternaam zorgprofessional
- AGB code zorgprofessional
- BIG code zorgprofessional
- Gebruikersnaam zorgprofessional
- E-mailadres zorgprofessional

Patiënt- en receptgegevens:

- Apotheek
- Naam praktijk
- Naam arts of verloskundige
- AGB code arts of verloskundige
- BIG code arts of verloskundige
- Adres Praktijk
- Postcode Praktijk
- Plaats Praktijk
- Gewenst bezorgadres (adres, postcode, plaats, land)
- Voorletters patiënt
- Achternaam patiënt
- Geboortedatum patiënt
- BSN nummer patiënt
- Mailadres patiënt
- Telefoonnummer patiënt
- Datum plaatsing IUD/implantaat
- Gebruikte omschrijving voorgeschreven (genees)middel
- Voor te schrijven (genees)middel
- Akkoord gegevens ophalen/delen met eigen apotheek via LSP
- Eventuele opmerkingen recept (o.a. conflicterend medicatiegebruik (ja/nee) of allergieën (ja/nee))

Subverwerkers voeren voor Verwerker de volgende Verwerkingen uit:

Subverwerkers verwerken in opdracht van Verwerker enkel de (bijzondere) persoonsgegevens als omschreven in deze Overeenkomst, te weten als hosting provider (CJ2) en ten behoeve van het verlenen van software onderhoud, development en support, alsmede het maken, opslaan en zo nodig terugzetten van back-ups, m.b.t. het Anticonceptieportaal en de doeleinden die daarmee redelijkerwijs samenhangen (MK2).

Annex 2

Specificatie van beveiliging subverwerkers

Subverwerker CJ2 (hosting)
De Deimten 11
9747 AV Groningen
info@cj2.nl
Om de beveiligingsstandaarden op hoog niveau in stand te houden maakt de Verwerker gebruik van de volgende zaken. Verwerker zal Verwerkingsverantwoordelijke informeren indien de hierna beschreven beveiligingsmaatregelen worden gewijzigd:

Fysieke beveiligingsmaatregelen hosting

- Alle persoonsgegevens worden opgeslagen op aparte servers die eigendom zijn van CJ2 (Sub-Verwerker, hosting) en die opgesteld staan in datacenters die gecertificeerd zijn conform ISO27001 en voldoen aan NEN 7510.
- De toegang tot dit datacenter is beperkt: slechts een drietal geregistreerde en gevalideerde medewerkers van subverwerker beschikken over toegangspassen en -codes.

Technische beveiligingsmaatregelen hosting

- De toegang tot de databases is beperkt tot een specifieke IP-reeks en kan enkel benaderd worden door een beperkt aantal technische medewerkers van subverwerker.
- De server van CJ2 met de persoonsgegevens kan niet van buitenaf worden benaderd. Uitgezonderd de eerder genoemde technische medewerkers.
- Alle informatie die wordt beheerd door CJ2 is beveiligd conform de ISO 27001 standaarden en NEN 7510.
- Alle webservices van de Verwerker zijn beveiligd met SSL certificaten.

De Back Office webservices zijn beveiligd met het EV SSL-certificaat (dit biedt het hoogste niveau van beveiliging voor authenticatie).

Subverwerker MK2 (onderhoud, ontwikkeling en support)

Bronsteeweg 49 a
2101 AB Heemstede
Support: 085 333 59 22 (What's app support)
Support: acp@mk2software.nl

Subverwerker is gecertificeerd volgens ISO 27001 en NEN 7510; de maatregelen zijn gebaseerd op ISO 27001 en NEN 7510. Om de beveiligingsstandaarden op hoog niveau in stand te houden hanteert Subverwerker de volgende maatregelen.

Organisatorische beveiligingsmaatregelen

1. Alle medewerkers van MK2 hebben een geheimhoudingsverplichting getekend, opgenomen in de arbeids- of opdrachtovereenkomst.
2. Toegang tot systemen en gegevens van het Anticonceptieportaal wordt uitsluitend verleend op basis van need-to-know en least privilege. Toegangsrechten worden bij in- en uitdiensttreding en bij functiewijziging aangepast; bij uitdiensttreding worden accounts dezelfde dag ingetrokken.
3. Toegang tot productiegegevens is beperkt tot zo min mogelijk medewerkers. Enkel medewerkers betrokken bij het project, of noodzakelijk zijn voor het uitvoeren van support, hebben toegang.

4. Ontwikkeling en testen vinden plaats in gescheiden omgevingen op gepseudonimiseerde of synthetische testdata. Productiegegevens worden niet gekopieerd naar ontwikkel- of testomgevingen en niet opgeslagen op werkstations van medewerkers.

5. Wijzigingen aan de software worden doorgevoerd via versiebeheer met code review door een tweede ontwikkelaar vóór uitrol naar productie.

6. Subverwerker hanteert een incidentprocedure: beveiligingsincidenten en (vermoedelijke) datalekken worden geregistreerd en binnen 4 uur na ontdekking gemeld aan Verwerker via support@softwarebv.nl en telefonisch aan een van de in de Afbakening genoemde contactpersonen van Verwerker.

7. Medewerkers krijgen elk kwartaal instructie over informatiebeveiliging en privacy (o.a. phishing, wachtwoordbeleid, omgang met patiëntgegevens).

8. Subverwerkers worden vooraf beoordeeld op beveiligingsniveau en contractueel gebonden aan ten minste dezelfde verplichtingen.

Technische beveiligingsmaatregelen

- **Toegang tot de omgeving van Verwerker:** Medewerkers loggen in op de servers via een beveiligde verbinding (SSH), met een persoonlijk account en een persoonlijke digitale sleutel. Er worden geen gedeelde accounts gebruikt, en de inloggegevens staan in een beveiligde wachtwoordkluis en worden nooit per mail of chat gedeeld.
- **Databasetoegang:** Slechts een klein aantal technische medewerkers mag bij de databases, en alleen via diezelfde beveiligde verbinding naar de server, nooit rechtstreeks vanaf een eigen laptop. Dit gebeurt alleen voor onderhoud, back-ups en het oplossen van storingen, en de toegang wordt ingetrokken zodra iemand niet meer aan het portaal werkt.
- **Omgang met productiegegevens:** De echte gegevens worden niet gedownload naar laptops, losse opslagmedia of clouddiensten van het bedrijf, behalve de back-ups. Onderzoek naar een storing gebeurt zoveel mogelijk op de server zelf. Is een export onvermijdelijk, dan gebeurt dat na overleg, versleuteld, en wordt de kopie meteen verwijderd.
- **Back-up en herstel:** Elke 12 uur wordt een versleutelde reservekopie gemaakt van de database en de bestanden. Die zijn alleen toegankelijk voor wie dat nodig heeft en worden 30 dagen bewaard. Bij herstel gaat hooguit 12 uur aan gegevens verloren en is het portaal binnen 24 uur weer beschikbaar.
- **Ontwikkeling en test:** Nieuwe functies worden gebouwd en getest met verzonnen of onherkenbaar gemaakte gegevens. Er wordt nooit een kopie van de echte database voor gebruikt.
- **Broncode en secrets:** De programmacode staat in een beveiligd systeem waarvoor je met een tweede inlogstap moet inloggen, en alleen de ontwikkelaars van het project hebben toegang. Wachtwoorden en andere geheime codes staan niet in de code zelf.
- **Wijzigingsbeheer:** Een wijziging wordt eerst op een aparte tak van de code gemaakt, daarna door een tweede ontwikkelaar beoordeeld en pas na akkoord van de opdrachtgever live gezet. Zo is altijd na te gaan wie wat wanneer heeft veranderd.
- **Secure development:** Er wordt gewerkt volgens de OWASP-richtlijnen, een bekende standaard voor veilig programmeren. Dat betekent onder meer dat ingevoerde gegevens gecontroleerd worden, dat bij elk verzoek wordt gecheckt of iemand wel bevoegd is, en dat er geen gevoelige gegevens in logbestanden of foutmeldingen komen. Gebruikte softwareonderdelen worden bijgewerkt als er een bekend beveiligingslek in zit, en de opdrachtgever wordt geadviseerd over updates van de serveromgeving.
- **Werkplekken van Subverwerker:** Alle laptops zijn versleuteld en beschermd met beveiligingssoftware die zichzelf bijwerkt. Medewerkersaccounts vragen altijd om een tweede inlogstap.
- **Logging:** Het bedrijf houdt bij wie toegang heeft tot de servers en legt elke ingreep op de echte omgeving vast (datum, wie, wat). Zo is bij een controle of incident altijd terug te vinden wat er is gebeurd.
- **Verwijdering:** Bij het einde van de samenwerking worden alle toegangen en sleutels ingetrokken. Ook de wachtwoorden in de kluis, de back-ups en eventuele lokale kopieën worden binnen 30 dagen verwijderd, en dat wordt schriftelijk bevestigd aan de opdrachtgever.