## Verwerkersovereenkomst – KiwiConnect

1. Toepasselijkheid, doel en reikwijdte

1.1 Doel. Deze verwerkersovereenkomst (de “Overeenkomst”) regelt de verwerking van Persoonsgegevens door Verwerker ten behoeve van Verwerkingsverantwoordelijke in het kader van het SaaS-platform voor skill-based matching, kandidaatbeheer, communicatie en bijbehorende analytics (de “Diensten”).

1.2 Relatie met hoofdovereenkomst. Deze Overeenkomst vormt een integrale bijlage bij de tussen Partijen gesloten hoofdovereenkomst(en). Bij strijdigheid prevaleert deze Overeenkomst voor zover het de verwerking van Persoonsgegevens betreft.

1.3 Reikwijdte verwerkingen. De aard, doeleinden, categorieën Persoonsgegevens en betrokkenen, verwerkingsactiviteiten, duur en bewaar-/retentietermijnen zijn gespecificeerd in Bijlage A (Verwerkingsdetails) en Bijlage B (Beveiligingsmaatregelen en retentie). Waar van toepassing worden subverwerkers en (potentiële) doorgiften opgenomen in Bijlage C (Subverwerkers & Doorgiften).

1.4 Instructies. Verwerker verwerkt Persoonsgegevens uitsluitend op gedocumenteerde instructie van Verwerkingsverantwoordelijke, tenzij een Unierechtelijke of lidstaatrechtelijke verplichting anders voorschrijft. In dat geval informeert Verwerker Verwerkingsverantwoordelijke vooraf, tenzij dit rechtens verboden is. Verwerker wijst Verwerkingsverantwoordelijke erop indien een instructie naar het oordeel van Verwerker in strijd is met toepasselijke wet- en regelgeving.

1.5 AI-functionaliteit (kader). Indien de Diensten (onderdelen van) AI-functionaliteit bevatten (zoals matching-modellen, scoringsalgoritmen of kwaliteitsverbetering), geldt: (i) training en verbetering vinden niet plaats op herleidbare Persoonsgegevens zonder afzonderlijke rechtsgrond of voorafgaande schriftelijke instructie; (ii) waar mogelijk wordt gewerkt met geaggregeerde, geanonimiseerde of anderszins onherleidbare data; (iii) rol- en plichtentoedeling onder de AVG en, zodra van toepassing, de EU AI-verordening, wordt nader uitgewerkt in Bijlage A (doeleinden, datasets, categorieën) en Bijlage B (technische/organisatorische maatregelen), met verwijzing naar risicobeheersing, data-governance en documentatie.

1.6 Territoriale scope & doorgifte. Verwerking vindt in beginsel plaats binnen de EU/EER. Doorgifte buiten de EU/EER is uitsluitend toegestaan met passende waarborgen (art. 46 AVG, waaronder EU-SCC’s), voorafgaande Transfer Impact Assessment en – indien nodig – aanvullende technische/contractuele maatregelen. Doorgiften en waarborgen worden opgenomen in Bijlage C; Verwerkingsverantwoordelijke wordt vooraf geïnformeerd en kan gemotiveerd bezwaar maken.

1.7 Hiërarchie en definities. Begrippen met hoofdletter hebben de betekenis uit de AVG; overige definities sluiten aan bij de hoofdovereenkomst en deze Overeenkomst. Bij strijdigheid tussen bijlagen en het hoofddeel van deze Overeenkomst geldt het hoofddeel.

2. Rolverdeling en verantwoordelijkheden

2.1 Rollen. Verwerkingsverantwoordelijke bepaalt de doeleinden en middelen van de verwerking en is verwerkingsverantwoordelijke in de zin van de AVG. Verwerker verwerkt Persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke en kwalificeert als verwerker. Partijen beogen geen gezamenlijke verwerkingsverantwoordelijkheid.

2.2 Verantwoordelijkheden Verwerkingsverantwoordelijke. Verwerkingsverantwoordelijke staat jegens Verwerker in voor: (i) rechtmatigheid van de verwerkingen (geschikte rechtsgrond, informatie-plichten, bewaartermijnen), (ii) juistheid en proportionaliteit van aangeleverde Persoonsgegevens (dataminimalisatie), (iii) het instrueren van Verwerker conform deze Overeenkomst, en (iv) – waar relevant – het uitvoeren van DPIA's en voorafgaande raadplegingen.

2.3 VerplichtingenVerwerker(kern). Verwerker: a) verwerkt uitsluitend op gedocumenteerde instructie van Verwerkingsverantwoordelijke; b) borgt dat alle personen die onder zijn verantwoordelijkheid Persoonsgegevens verwerken aan passende (contractuele) geheimhouding zijn gebonden; c) treft passende technische en organisatorische maatregelen (TOM's) zoals uitgewerkt in Bijlage B en houdt een register van verwerkingsactiviteiten bij; d) assisteert Verwerkingsverantwoordelijke – voor zover mogelijk – bij het nakomen van verplichtingen t.a.v. rechten van betrokkenen, beveiliging, meldplichten datalekken, DPIA's en voorafgaande raadpleging; e) faciliteert audits conform artikel 11 (Audit en Inspectie) en verstrekt redelijke informatie ter onderbouwing van compliance; f) onthoudt zich van (her)gebruik voor eigen doeleinden, profiling of geautomatiseerde besluitvorming met rechtsgevolg buiten de instructies van Verwerkingsverantwoordelijke; g) activeert procedures voor tijdige datalek-melding en incidentrespons zoals nader beschreven in artikel 8 en Bijlage D.

2.4 AI-specifieke rolafbakening (samenvatting). Voor zover Verwerker (delen van) AI-functionaliteit levert binnen de Diensten, waarborgt Verwerker dat: (i) datasets en features binnen de overeengekomen doeleinden blijven, (ii) bias-reducerende maatregelen en kwaliteitscontroles onderdeel zijn van het ontwikkel- en vrijgaveproces, (iii) geen re-identificatie plaatsvindt van geanonimiseerde/aggregaatdata, en (iv) documentatie over modeldoel, inputcategorieën en evaluatie op verzoek beschikbaar is voor audit/assurance. Nadere technische invulling volgt in Bijlage A/B.

2.5 Afwijkende instructies en wettelijk bevel. Indien een instructie onverenigbaar is met toepasselijk recht, meldt Verwerker dit onverwijld. Bij een wettelijk bevel (bijv. toezicht/handhaving) verstrekt Verwerker uitsluitend de minimaal vereiste gegevens, toetst de rechtmatigheid, en informeert Verwerkingsverantwoordelijke vooraf, voor zover toegestaan.

3. Verwerkingsdetails

3.1 Overzicht. De aard, doeleinden, duur, categorieën persoonsgegevens en betrokkenen zijn gespecificeerd in Bijlage A (Verwerkingsdetails). Dit artikel vat de kernafspraken samen en voegt beheersmaatregelen toe die voor de uitvoering essentieel zijn.

3.2 Aard van de verwerkingen. Verwerkingen omvatten (afhankelijk van de geactiveerde modules): verzamelen, ontvangen, vastleggen, ordenen, structureren, opslaan (inclusief back-ups), bewerken/wijzigen, raadplegen, analyseren (matching/scoring), combineren, pseudonimiseren, beperken, verstrekken via geautoriseerde weergave/export en verwijderen. De concrete handelingen en datastromen worden per module in Bijlage A benoemd.

3.3 Doeleinden. De Diensten zien op: (i) skill-based matching en (voor)selectie, (ii) kandidaatbeheer en communicatie, (iii) rapportage en kwaliteitsverbetering van matching, (iv) beveiliging, logging en misbruikdetectie. Verwerker verwerkt uitsluitend voor deze doeleinden en conform de gedocumenteerde instructies van Verantwoordelijke.

3.4 Duur en retentie. De verwerkingen lopen gedurende de contractduur. Retentie (inclusief log- en back-uprotaties) is nader uitgewerkt in Bijlage B (Beveiligingsmaatregelen & retentie); bij beëindiging gelden de procedures van artikel 12 (teruggave/verwijdering).
3.5 Categorieën betrokkenen. Kandidaten/sollicitanten; (contactpersonen van) recruiters/hiring managers; referenten indien aangeleverd door Verantwoordelijke of kandidaat.

3.6 Categorieën persoonsgegevens. Identificatie- en contactgegevens; professionele gegevens (cv, opleiding, werkervaring, vaardigheden/competenties, beschikbaarheid, portfolio); matchingdata (scores, tags, notities, feedback); technische gebruiksdata (account-ID's, loggegevens, IP-adres, user-agent). Opmerking over beelden: indien Verantwoordelijke cv's of profielen met foto aanlevert, valt dit binnen de categorie "beeldmateriaal"; Verantwoordelijke staat in voor een passende rechtsgrond en transparantie richting betrokkenen.

3.7 Bijzondere categorieën. Verwerker beoogt géén verwerking van bijzondere categorieën. Indien dergelijke gegevens toch door Verantwoordelijke worden aangeleverd (bijvoorbeeld via open tekstvelden of foto's waaruit bijzondere gegevens kunnen blijken), gebeurt verwerking uitsluitend onder diens verantwoordelijkheid en met passende waarborgen (pseudonimisatie, toegangsbescherming) zoals nader beschreven in Bijlage B.

3.8 Rechtsgrond & informatieplicht. De rechtsgrond, informatieverstrekking en uitoefening van rechten van betrokkenen berusten bij Verantwoordelijke. Verwerker ondersteunt conform artikel 9 en Bijlage D (Contactpunten & procedures).

3.9 AI-functionaliteit (datagebruik en begrenzing). Voor AI-ondersteunde functies (matching/scoring, kwaliteitsverbetering) geldt: a) Modeltraining en -tuning op herleidbare persoonsgegevens vindt niet plaats zonder schriftelijke instructie en passende waarborgen; b) Waar mogelijk wordt gewerkt met geanonimiseerde of onherleidbaar geaggregeerde datasets; c) Modeldocumentatie (doel, inputcategorieën, evaluatiecriteria, bias-reductiemaatregelen) is op verzoek beschikbaar voor audit/assurance; d) Data wordt niet gebruikt voor algemene modelverbetering buiten de overeengekomen doeleinden zonder aanvullende afspraak in Bijlage A. Deze uitgangspunten worden expliciet in Bijlage A opgenomen, met technische invulling in Bijlage B.

3.10 Doorgiften en subverwerkers. Locaties van verwerking en subverwerkers (incl. doorgifte-grondslag buiten EU/EER) staan in Bijlage C. Wijzigingen volgen de notificatie- en bezwaarprocedure van artikel 5.

4. Verplichtingen van Verwerker

4.1 Geheimhouding. Verwerker waarborgt dat medewerkers en ingeschakelde hulppersonen die toegang hebben tot persoonsgegevens contractueel tot vertrouwelijkheid zijn verplicht en adequaat zijn geïnstrueerd over beveiliging en privacy.

4.2 Doelbinding en instructies. Verwerker verwerkt uitsluitend op gedocumenteerde instructie van Verantwoordelijke en onthoudt zich van verwerking voor eigen doeleinden (inclusief profiling met rechtsgevolg) tenzij wettelijk verplicht; in dat geval informeert Verwerker Verantwoordelijke vooraf, voor zover rechtens toegestaan.

4.3 Technische en organisatorische maatregelen (TOM’s). Verwerker treft passende TOM’s, waaronder ten minste: rolgebaseerde autorisaties en least-privilege, MFA voor beheerders, encryptie in transit en at rest waar passend, netwerk-segregatie, beveiligde softwareontwikkelcyclus (inclusief code-review en dependency-scans), logging/monitoring, vulnerability- en patch-management, back-up & hersteltests, change- en incidentmanagement, periodieke access-reviews en supplier-due-diligence. De actuele uitwerking en retentieschema’s staan in Bijlage B.

4.4 Register en compliance-informatie. Verwerker houdt een register van categorieën van verwerkingsactiviteiten bij en verstrekt op verzoek relevante informatie (assurance-rapporten, security-assessments, samenvattingen van penetratietesten) om compliance aan te tonen, met inachtneming van vertrouwelijkheid. Dit laat het auditrecht van artikel 11 onverlet.

4.5 Ondersteuning bij rechten van betrokkenen. Verwerker faciliteert Verantwoordelijke, voor zover technisch mogelijk binnen de Diensten, bij verzoeken ex. AVG (inzage, rectificatie, wissing, beperking, dataportabiliteit, bezwaar) binnen redelijke termijnen en volgens het proces in Bijlage D. Werkzaamheden buiten reguliere support kunnen op basis van redelijke, vooraf gecommuniceerde kosten worden uitgevoerd.

4.6 DPIA en voorafgaande raadpleging. Op verzoek verleent Verwerker medewerking aan DPIA's en (indien van toepassing) voorafgaande raadplegingen bij de toezichthouder; Verwerker levert relevante technische en organisatorische informatie aan en implementeert in redelijkheid overeengekomen mitigerende maatregelen.

4.7 Overheids- en handhavingsverzoeken. Verwerker verstrekt uitsluitend de minimaal vereiste informatie, beoordeelt de rechtmatigheid van het verzoek en informeert Verantwoordelijke vooraf, tenzij dit rechtens verboden is. Verwerker documenteert de afhandeling.

4.8 Incident- en datalekmanagement. Verwerker onderhoudt procedures voor detectie, triage, mitigatie en melding van inbreuken; Verwerker meldt onverwijld conform artikel 8 en levert alle informatie die Verantwoordelijke nodig heeft voor eventuele meldingen aan toezichthouders en betrokkenen.

4.9 Subverwerkers. Inschakeling van subverwerkers geschiedt conform artikel 5; Verwerker legt minimaal gelijkwaardige verplichtingen op en blijft volledig aansprakelijk voor hun handelen. Overzicht en wijzigingen: Bijlage C.

4.10 Gebruik voor kwaliteitsverbetering. Verwerker mag uitsluitend geanonimiseerde/onherleidbaar geaggregeerdegegevens gebruiken voor statistiek, beveiliging en kwaliteitsverbetering. Re-identificatie is verboden. Modeltraining op persoonsgegevens geschiedt alleen met aparte instructie/rechtsgrond en wordt expliciet vastgelegd in Bijlage A.

4.11 Continuïteit en exit. Verwerker handhaaft passende continuïteitsmaatregelen (back-ups, herstelplannen). Bij beëindiging assisteert Verwerker bij ordentelijke overdracht; teruggave/verwijdering conform artikel 12 en Bijlage B(uitfaseringsschema back-ups).

5. Subverwerkers

5.1 Algemene machtiging + meldplicht. Verwerker is bevoegd subverwerkers in te schakelen, mits zij ten minste gelijkwaardige privacy- en beveiligingsverplichtingen opgelegd krijgen als in deze Overeenkomst. Verwerker informeert Verwerkingsverantwoordelijke vooraf schriftelijk over voorgenomen wijzigingen in de subverwerkerslijst (Bijlage C) met een toelichting op rol, locatie en waarborgen; Verwerkingsverantwoordelijke kan binnen 30 dagen gemotiveerd bezwaar maken. Bij urgentie (business continuity) kan Verwerker tijdelijk inschakelen met een verkorte meldtermijn, mits zo spoedig mogelijk volledig geïnformeerd wordt.

5.2 Flow-down verplichtingen en toezicht. Verwerker legt subverwerkers minimaal dezelfde (of strengere) contractuele verplichtingen op als tussen Partijen gelden, inclusief geheimhouding, TOM's, audit/assurance, datalekprocessen, AI-datagebruikbeperkingen en doorgifte-waarborgen. Verwerker toetst vooraf en periodiek (redelijkerwijs) de naleving, documenteert die toetsing en verstrekt op verzoek een samenvatting van relevante afspraken met subverwerkers.

5.3 Aansprakelijkheid. Verwerker blijft volledig verantwoordelijk voor de handelingen en nalatigheden van subverwerkers als voor eigen handelen. Eventuele aansprakelijkheidsafspraken uit de hoofdovereenkomst gelden mutatis mutandis, met inachtneming van het verbod op exoneratie voor verlies/verwerking van Persoonsgegevens in strijd met deze Overeenkomst voor zover dat aan Verwerker/subverwerker toerekenbaar is.

5.4 AI-specifieke eisen aan subverwerkers. Indien een subverwerker AI-functionaliteit levert (bijv. matching, scoring, filtering of monitoring): (i) geen training of fine-tuning op herleidbare Persoonsgegevens zonder schriftelijke instructie; (ii) waar mogelijk uitsluitend geanonimiseerde of onherleidbare aggregaten; (iii) documentatie over modeldoel, inputcategorieën, evaluaties en bias-reductie beschikbaar voor audit/assurance; (iv) verbod op re-identificatie; (v) duidelijke data-retentie en delete-procedures. Deze voorwaarden worden in Bijlage C geborgd per subverwerker.

5.5 Bezwaar en alternatieven. Bij tijdig en gemotiveerd bezwaar werkt Verwerker in redelijkheid mee aan een passend alternatief (zoals een andere subverwerker, configuratiewijziging of datalokaliseer-oplossing). Indien geen alternatief haalbaar is, kan Verwerkingsverantwoordelijke het betreffende onderdeel van de Diensten beëindigen zonder boete; eventuele vooruitbetaalde vergoedingen voor dat onderdeel worden naar rato gecrediteerd.

5.6 Transparantie en actualiteit Bijlage C. Verwerker houdt Bijlage C actueel met per subverwerker: naam, rol, verwerkingslocatie, (potentiële) doorgifte, grondslag/waarborg (bijv. SCC's), TIA-status en belangrijkste technische/organisatorische maatregelen. Remote support/toegang van personeel buiten de EER wordt als (potentiële) doorgifte zichtbaar gemaakt.

6. Doorgifte buiten de EU/EER (Schrems II)

6.1 EU/EER als uitgangspunt. Verwerking vindt in beginsel plaats binnen de EU/EER. Doorgifte buiten de EU/EER (waaronder remote toegang door support- of operations-personeel buiten de EER) is alleen toegestaan indien passende waarborgen ex art. 46 AVG aanwezig zijn en voorafgaand een Transfer Impact Assessment ("TIA") is uitgevoerd. Doorgiften en waarborgen worden opgenomen in Bijlage C.

6.2 Waarborgen en TIA. Indien doorgifte noodzakelijk is, past Verwerker passende waarborgen toe (zoals EU-SCC's) en beoordeelt – met inachtneming van het toepasselijke recht in het derde land – of aanvullende maatregelen vereist zijn, waaronder (voor zover passend): (i) sterke end-to-end-encryptie met sleutelbeheer binnen de EU onder exclusieve controle van Verwerker of een EU-trustee; (ii) dataminimalisatie/pseudonimisering met sleutelgescheidenheid; (iii) strikte toegangscontrole, logging en just-in-time access; (iv) contractuele beperkingen op overheidsverzoeken en transparantierapportage. Indien adequate bescherming niet kan worden geborgd, wordt de doorgifte opgeschort.

6.3 Max Schrems/ontwikkelingen en herbeoordeling. Verwerker volgt juridische ontwikkelingen (zoals procedures over het EU-US adequaatheidsbesluit) en herbeoordeelt periodiek de TIA's en waarborgen. Bij materiële wijzigingen die de doorgifte-grondslag of het risicoprofiel beïnvloeden, informeert Verwerker Verwerkingsverantwoordelijke onverwijld met een voorstel voor mitigerende maatregelen of een exit-scenario (migratie naar EU-alternatieven).

6.4 Ketenverantwoordelijkheid. Verwerker waarborgt dat elke subverwerker met (potentiële) toegang buiten de EU/EER eveneens voldoet aan 6.2 (SCC's, TIA en aanvullende maatregelen). Verwerker documenteert keten-doorgiften en stelt op verzoek een samenvatting van TIA-uitkomsten beschikbaar, met behoud van vertrouwelijkheid.

6.5 Informatieplicht en bezwaar. Verwerker informeert Verwerkingsverantwoordelijke vooraf over nieuwe doorgiften of materiële wijzigingen in bestaande doorgiften (bijv. wijziging verwerkingslocatie of supportmodel). Verwerkingsverantwoordelijke kan gemotiveerd bezwaar maken; Verwerker werkt dan in redelijkheid mee aan een alternatief of – indien niet haalbaar – beëindiging van het betreffende onderdeel zonder boete (pro rata restitutie).

6.6 Overheidsverzoeken. Bij verzoeken van autoriteiten buiten de EU/EER verstrekt Verwerker uitsluitend de minimaal vereiste gegevens, toetst de rechtmatigheid, en informeert Verwerkingsverantwoordelijke vooraf, tenzij dit rechtens verboden is. Verwerker documenteert het verzoek en de afhandeling en past – waar toegestaan – transparantie- en weerstandsbepalingen toe.

6.7 AI-datagebruik bij doorgifte. AI-gerelateerd datagebruik (trainen/tunen, evaluatie, monitoring) valt niet onder doorgifte-grondslagen voor algemene modelverbetering, tenzij uitdrukkelijk overeengekomen in Bijlage A met passende waarborgen en (waar nodig) toestemming of een andere rechtsgrond; anderszins wordt uitsluitend met geanonimiseerde/onherleidbare aggregaten gewerkt.

7. Bewaartermijnen en dataminimalisatie

7.1 Principe. Verwerker verwerkt niet méér gegevens en niet langer dan nodig. Verantwoordelijke bepaalt de (module-specifieke) termijnen; Verwerker faciliteert en afdwingt die termijnen technisch.

7.2 Standaardtermijnen. a) Kandidaatgegevens (profiel, cv, notities, matching): 12 maanden na laatste activiteit, daarna anonimisering of verwijdering. b) Klantgebruik/logging (app- en auditlogs): 180 dagen; security-logs 12 maanden. c) Supporttickets en bijlagen: 24 maanden na sluiting. d) Back-ups: rolling schema (bijv. 35 dagen), uitsluitend voor herstel; geen productietoegang. e) Exports/downloads: 14 dagen retentie in versleutelde tijdelijke opslag, daarna automatische verwijdering. Afwijkingen worden vastgelegd in Bijlage B (Beveiliging & Retentie).

7.3 Anonimiseren vs. verwijderen. Waar operationeel zinvol anonimiseert Verwerker (onherleidbaar) ten behoeve van kwaliteitsbewaking/statistiek. Op instructie kan “hard delete” worden toegepast; in back-ups blijft herstel tot afloop van de back-upcyclus mogelijk. Re-identificatie is verboden.

7.4 Dataminimalisatie by design. a) Alleen noodzakelijke velden; vrije tekstvelden zijn uit te schakelen of te beperken. b) Technische beperkingen op bulk-uploads en bijlagen (type/omvang). c) Automatische detectie/waarschuwing bij mogelijke invoer van bijzondere categorieën.

7.5 Configuratie & bewijs. Verantwoordelijke kan per workflow retenties instellen (policy-profielen). Verwerker logt het toepassen van retenties en kan rapporteren voor audits.

7.6 Rechten van betrokkenen. Bij een geldig verwijderingsverzoek verwijdert Verwerker productie-data zonder onredelijke vertraging. In back-ups wordt een tombstone/suppress-record toegepast om herintroductie bij herstel te voorkomen.

7.7 Datareductie en transparantie bij AI-functies a) Dataminimalisatie. Datasets die worden gebruikt voor matching- of scoringsfunctionaliteiten worden zodanig ingericht dat alleen gegevens worden verwerkt die aantoonbaar bijdragen aan het beoogde modeldoel. Overbodige velden worden uitgesloten of geanonimiseerd. b) Pseudonimisering. Persoonsgegevens worden vóór gebruik in AI-processen gepseudonimiseerd zodat ze niet direct tot natuurlijke personen herleidbaar zijn. Sleutels worden afzonderlijk en beveiligd bewaard. c) Transparantie en uitlegbaarheid. Verwerker legt in begrijpelijke taal uit welke gegevenscategorieën worden gebruikt, hoe de verwerking plaatsvindt, en welke factoren invloed hebben op de gegenereerde score of ranking. Deze uitleg wordt in een korte toelichting (max. 2 pagina’s) beschikbaar gesteld aan de Verwerkingsverantwoordelijke. d) Geen training op herleidbare data. Er vindt geen training of fine-tuning plaats op datasets die Persoonsgegevens bevatten, tenzij daarvoor een schriftelijke instructie is gegeven en een passende rechtsgrond aanwezig is (zie Bijlage A en B). e) Beperkingen en controles. Verwerker controleert periodiek of gebruikte datasets voldoen aan beginselen van dataminimalisatie, fairness en proportionaliteit, en documenteert deze toetsing.

8. Inbreuken (datalekken) & incidentrespons

8.1 Definities. a) Beveiligingsincident Elke gebeurtenis – technisch, organisatorisch of menselijk – die de vertrouwelijkheid, integriteit of beschikbaarheidvan Persoonsgegevens of informatiesystemen kan aantasten. Voorbeelden hiervan zijn:

• onbevoegde of mislukte pogingen tot toegang; • verlies of vernietiging van gegevens door fout, storing of malware; • misbruik van toegangsrechten of wachtwoorden; • uitval of incorrecte werking van beveiligingsmaatregelen (encryptie, authenticatie, logging). b) Inbreuk in verband met Persoonsgegevens (“datalek”) Een beveiligingsincident dat leidt tot ongeoorloofde of onbedoelde toegang, openbaarmaking, wijziging, verlies of vernietiging van Persoonsgegevens. Een datalek kan zowel ontstaan door menselijke fouten (bijv. verkeerd geadresseerde e-mail, verloren laptop) als door technische of kwaadaardige

oorzaken (hacken, ransomware, softwarefout). c) Juridisch kader De begrippen sluiten aan op de definities van artikel 4, onderdeel 12 AVG en de richtsnoeren van de Europese Toezichthouders (EDPB 01/2021). Verwerker volgt deze wetgeving en handelt conform de meldplichten van artikelen 33 en 34 AVG en de Nederlandse Uitvoeringswet AVG. d) Reikwijdte Onder deze definities vallen ook incidenten binnen AI-functionaliteit, waaronder fouten in modelconfiguratie, verkeerde datasets of onbedoelde herleidbaarheid van trainingsdata. Zodra hierdoor Persoonsgegevens (mogelijk) worden blootgesteld of misbruikt, kwalificeert dit als een datalek in de zin van dit artikel.

8.2 Detectie & monitoring. Verwerker onderhoudt 24/7 monitoring, logging en alertering op kritieke systemen. Onder kritieke systemen worden verstaan: – productieomgevingen waarin Persoonsgegevens worden verwerkt of opgeslagen; – de centrale databases en API-knooppunten die toegang geven tot deze gegevens; – authenticatie- en autorisapeservices (identity management, SSO, MFA); – opslag- en back-upsystemen die nodig zijn voor conpnuïteit en herstel; – netwerk- en cloudcomponenten die de beschikbaarheid van de Diensten waarborgen. Voor deze systemen gelden vooraf ingestelde drempelwaarden voor verdachte activiteiten, waaronder pogingen tot ongeautoriseerde toegang, privilege-escalatie, massale data-export of wijziging van beveiligingsinstellingen. Fout- en beveiligingsmeldingen worden centraal gecorreleerd in een Security Information & Event Management-platform (SIEM) of gelijkwaardige oplossing, zodat detectie en incidentrespons tijdig plaatsvinden.

8.3 Meldplicht aan Verantwoordelijke Verwerker meldt een vermoedelijk datalek onverwijld en zonder onredelijke vertraging, in beginsel binnen 24 uur na ontdekking, met minimaal: a) aard van de inbreuk (categorie, systemen, tijdlijn), b) vermoedelijke omvang en categorieën van gegevens en betrokkenen, c) (voorlopige) oorzaak en getroffen beveiligingsmaatregelen, d) reeds genomen of voorgestelde mitigerende stappen, e) contactpunt voor incidentrespons. Updates volgen op vaste intervallen totdat het incident is afgesloten. Verwerker handelt hierbij conform de meldplichten uit artikelen 33 en 34 van de Algemene Verordening Gegevensbescherming (AVG) en de richtlijnen van de Autoriteit Persoonsgegevens.

8.4 Ondersteuning meldingen AP/betrokkenen Verwerker levert alle informatie die de Verwerkingsverantwoordelijke nodig heeft om – waar vereist – melding te doen bij de toezichthouder of de betrokkenen, waaronder risicobeoordelingen, voorbeeldteksten en communicatievoorstellen. Verwerker verzendt zelf geen meldingen namens Verwerkingsverantwoordelijke, tenzij dit schriftelijk is opgedragen.

8.5 Beperking en herstel Verwerker treft onmiddellijk maatregelen om het incident te isoleren en verdere schade te voorkomen, waaronder toegangsintrekking, sleutelrotatie, blokkade van uitgaande datastromen en noodpatching. Back-up- en herstelprocedures worden waar nodig geactiveerd om continuïteit te waarborgen.

8.6 Forensics en bewijspreservatie Alle relevante systeem- en applicatielogs, geheugen-dumps en configuraties worden veiliggesteld en voorzien van een integriteitscontrole (hashing). Indien externe forensische ondersteuning wordt ingezet, blijft geheimhouding geborgd en wordt de keten van bewaring vastgelegd.

8.7 Root Cause Analysis (RCA) Binnen 30 dagen na containment levert Verwerker een rapport met de oorzaak, impact, verbetermaatregelen en lessen voor de toekomst. Het verbeterplan bevat tijdsgebonden acties met technische en organisatorische maatregelen.

8.8 Communicatiekaders Externe communicatie richting pers of klanten van de Verwerkingsverantwoordelijke vindt uitsluitend plaats in overleg en afstemming met Verwerkingsverantwoordelijke. Openbare verklaringen worden vooraf goedgekeurd, tenzij wet of bevel anders vereist. 8.9 Subverwerkers Indien Verwerker subverwerkers inzet, gelden voor hen gelijke meld- en medewerkingsplichten. De subverwerker verstrekt onverwijld alle relevante informatie en loggegevens aan Verwerker om de ketenrespons te coördineren en tijdige melding aan de Verwerkingsverantwoordelijke te waarborgen.

9. Rechten van betrokkenen & verzoekafhandeling

9.1 Rolverdeling. Verwerkingsverantwoordelijke is primair aanspreekpunt voor betrokkenen. Verwerker ondersteunt “voor zover mogelijk” met functies, exporten en bewerkingen binnen de Diensten.

9.2 Kanaal & ontvangst. Verzoeken die bij Verwerker binnenkomen, worden onverwijld doorgestuurd naar het door Verantwoordelijke opgegeven contactpunt. Verwerker bevestigt ontvangst richting Verantwoordelijke met datum/tijd en een korte samenvatting van het verzoek.

9.3 Identiteitsvaststelling. Verwerker faciliteert verificatie door (i) gecontroleerde login, of (ii) een beperking tot dossier-/accountdata onder beheer van Verantwoordelijke. Verwerker verwerkt geen extra identiteitsdocumenten, tenzij schriftelijk opgedragen met passende waarborgen.

9.4 Termijnen. Verwerker levert de benodigde ondersteuning zó dat Verantwoordelijke binnen de AVG-termijnen kan handelen (richtsnoer: initiële reactie binnen 7 dagen; afronding in de regel binnen 30 dagen, verlengbaar waar toegestaan).

9.5 Type verzoeken en uitvoering Verwerker ondersteunt de Verwerkingsverantwoordelijke bij de afhandeling van verzoeken van betrokkenen overeenkomstig de artikelen 12 tot en met 22 van de Algemene Verordening Gegevensbescherming (AVG). De uitvoering sluit aan bij de gangbare praktijk en wettelijke termijnen binnen de AVG. a) Inzage en dataportabiliteit Betrokkenen hebben recht op inzage en overdraagbaarheid van hun persoonsgegevens. Verwerker faciliteert een machine-leesbare export (bijvoorbeeld JSON of CSV) van de persoonsgegevens die op de betrokkene betrekking hebben, inclusief de voor zover redelijk beschikbare metadata. Bedrijfsgevoelige informatie of interne notities worden niet verstrekt. b) Rectificatie

Verwerker past op instructie van de Verwerkingsverantwoordelijke uitsluitend de aangewezen velden aan. Elke wijziging wordt gelogd zodat controleerbaar blijft wat is aangepast. c) Wissing (“recht op vergetelheid”) Verwerker verwijdert of anonimiseert persoonsgegevens conform de vastgelegde retentie-instellingen. Indien volledige verwijdering tijdelijk niet mogelijk is (bijvoorbeeld in back-ups), wordt een suppress-record toegepast om herintroductie te voorkomen. d) Beperking van verwerking Verwerker markeert de betreffende persoonsgegevens met een statusflag waardoor verdere verwerking, export of rapportage wordt geblokkeerd. De naleving hiervan wordt periodiek gecontroleerd. e) Bezwaar of opt-out Verwerker sluit betrokkenen op verzoek uit van niet-noodzakelijke of facultatieve verwerkingen, zoals rapportages of analyses die niet strikt noodzakelijk zijn voor de uitvoering van de Diensten. f) Geautomatiseerde besluitvorming en profilering Op verzoek verstrekt Verwerker via de Verwerkingsverantwoordelijke uitleg over het logische verloop van de relevante geautomatiseerde verwerking, inclusief de betrokken factoren en de mogelijkheid van menselijke tussenkomst, conform artikel 22 AVG.

9.6 Uitzonderingen. Verwerker signaleert wanneer verzoeken (deels) niet uitvoerbaar zijn wegens wettelijke verplichtingen, rechten van derden of bedrijfsgeheimen. Verantwoordelijke beslist; Verwerker voert uit volgens instructie.

9.7 Kosten & prioriteit. Normale ondersteuning valt onder de Diensten. Substantiële, maatwerk-inspanningen gebeuren op redelijke, vooraf gecommuniceerde tarieven, behalve als de noodzaak voortvloeit uit toerekenbaar handelen van Verwerker of subverwerker.

9.8 Audittrail. Verwerker registreert per verzoek: tijdlijn, uitgevoerde stappen, verantwoordelijke accounts en uitkomst. Rapportage is op verzoek beschikbaar.

10. Beveiliging – Technische en organisatorische maatregelen (TOM’s) (Dit artikel specificeert de maatregelen; het herhaalt geen bepalingen over doelbinding, meldplichten of subverwerkers.)

10.1 Governance & beleid. a) Vastgestelde security- en privacy-policies (jaarlijks herzien). b) Rollen en verantwoordelijkheden (CISO/ISO-functie, DPO-koppelpunt). c) Verplichte security- en privacy-training (minimaal jaarlijks; onboarding vooraf). d) Screenings- en geheimhoudingsverplichtingen voor medewerkers met toegang.

10.2 Toegangsbeheer. a) Identity-first: individuele accounts, geen gedeelde productietoegang. b) Least-privilege & need-to-know, periodieke access reviews (min. per kwartaal). c) Sterke authenticatie (MFA) voor beheerfuncties en externe toegang. d) Just-in-time en time-boxed elevatie voor productie-toegang; volledige logging.

10.3 Cryptografie & sleutelbeheer. a) Data in transit via TLS 1.2+; HSTS aan de front-ends. b) Data at rest versleuteld met moderne algoritmes; sleutelrotatie volgens schema. c) Gescheiden key-stores; beperkte sleuteltoegang; key-events gelogd.

10.4 Netwerk- & platformbeveiliging. a) Segregatie van omgevingen (dev/test/acceptatie/productie). b) Ingress/egress-controle, WAF, rate-limiting en DDoS-bescherming. c) Patch-management met risicogebaseerde deadlines; hardening-baselines.

10.5 Applicatie-beveiliging (SDLC). a) Secure coding-normen; verplichte peer code-review. b) Dependency-scanning (SCA) en SAST in CI; periodieke DAST/pen-tests. c) Geheimenbeheer via een secrets-manager; geen secrets in code/CI-logs. d) Change-management met vier-ogenprincipe; rollback-procedures.

10.6 Dataclassificatie & -segregatie. a) Classificatie (bijv. publiek / intern / vertrouwelijk / persoonsgegeven). b) Logische tenant-isolatie; testdata is geanonimiseerd of synthetisch. c) Beperkingen op vrije tekstvelden en bijlagen (file-type, AV-scan, size-limits).

10.7 Back-ups & herstel/continuïteit. a) Versleutelde back-ups, geografisch gespreid binnen afgesproken regio('s). b) Hersteloefeningen (min. 2× per jaar) met RPO/RTO-rapportage. c) Runbooks voor uitwijk; afhankelijkheden en contactpunten gedocumenteerd.

10.8 Kwetsbaarheden & derde partijen. a) Gepland vuln-management (CVE-feed, prioritering op CVSS/EPSS + exploitability). b) Leveranciers-due-diligence vooraf en periodiek; contractuele security-clausules.

10.9 Fysieke en cloud-security. a) Datacenters met certificeringen (bijv. ISO 27001/SOC-rapporten van de provider). b) Strikt role-based datacenter-toegangsbeleid (door cloudprovider); auditsamenvattingen beschikbaar. c) Beperkingen op offline exports; versleutelde stations op beheerderslaptops.

10.10 Privacy by design & by default. a) Dataminimalisatie in formulieren, API's en exports. b) Pseudonimisering van datasets voor analyses en modelontwikkeling. c) Configurabele retentie-policies en standaard "privacy-vriendelijke" defaults.

10.11 AI-specifieke waarborgen (aanvullend). a) Model-kaart (doel, inputs, evaluatiemetrics, drift-monitoring, gebruiksbeperkingen). b) Strikte scheiding tussen productie-persoonsgegevens en trainingscorpora; waar mogelijk uitsluitend geanonimiseerde/gesynthetiseerde data. c) Model-versiebeheer en reproduceerbaarheid van scores; explainability-info beschikbaar in beheerkanalen. d) Verboten: re-identificatie en hergebruik van herleidbare persoonsgegevens voor algemene modelverbetering zonder expliciete instructie en rechtsgrond.

10.12 Bekendmaking & assurance. a) Op verzoek: samenvattingen van relevante assurance-rapporten (bijv. ISO/SOC, pen-tests). b) Bevindingen uit audits/oefeningen worden opgevolgd met tijdgebonden maatregelen en voortgangsrapportage.

11. Audit & inspectie

11.1 Reikwijdte. Audit ziet uitsluitend op naleving van deze verwerkersovereenkomst en relevante AVG-verplichtingen. Bedrijfsgeheimen, broncode en prijzen vallen erbuiten, tenzij strikt noodzakelijk om naleving aan te tonen.

11.2 Volgorde van bewijslast (tiered). a) Eerst: door Verwerker beschikbaar gestelde bewijsstukken (ISO/SOC-samenvattingen, pen-test-samenvattingen, policy-overzichten, access-review logs). b) Vervolgens (indien onvoldoende): remote document-/interviewaudit. c) Pas als dat nog onvoldoende is: onsite audit onder begeleiding van Verwerker.

11.3 Frequentie & aankondiging. Maximaal 1 audit per 12 maanden en bij een redelijk vermoeden van materiële non-compliance of incident. Aankondiging minimaal 10 werkdagen vooraf, met auditplan (scope, vragenlijst, benodigde personen).

11.4 Verloop. Audits worden uitgevoerd binnen kantooruren, zonder productie te verstoren, en volgens het need-to-know-principe. Verwerker kan redelijke beperkingen stellen (veiligheid, continuïteit, privacy van andere klanten).

11.5 Derden & geheimhouding. Auditoren tekenen vooraf een NDA. Verwerker mag een auditor weigeren bij redelijke objectie (bijv. directe concurrent of belangenconflict); Verantwoordelijke wijst dan een gelijkwaardig alternatief aan.

11.6 Beperkingen. Geen penetratietesten of scans tegen productie zonder voorafgaande schriftelijke afstemming over scope, tijdvensters en stop-condities. Testdata is geanonimiseerd of synthetisch.

11.7 Uitkomsten & herstel. Bevindingen worden door Partijen besproken binnen 10 werkdagen na het auditrapport. Verwerker levert een verbeterplan met maatregelen en termijnen passend bij de ernst (bijv. P1 binnen 14 dagen).

11.8 Kosten. Kosten van audits zijn voor Verantwoordelijke, tenzij (i) een materiële schending door Verwerker of subverwerker wordt vastgesteld, of (ii) Verwerker verplichte bewijsstukken niet kon leveren; in die gevallen draagt Verwerker de redelijke auditkosten.

12. Einde dienstverlening: teruggave, verwijdering & exit-support

12.1 Triggers. Beëindiging kan plaatsvinden door afloop, opzegging of ontbinding van de hoofdovereenkomst, of bij (gedeeltelijke) beëindiging van specifieke modules.

12.2 Teruggave op verzoek. Verantwoordelijke kan gedurende 30 dagen na beëindiging kosteloos één volledige data-export opvragen (JSON/CSV + bestand-bijlagen), inclusief een schema-overzicht van de datavelden. Extra of maatwerk-exports zijn mogelijk op basis van redelijke tarieven.

12.3 Verwijdering. Na afloop van de exporttermijn verwijdert Verwerker Persoonsgegevens uit productieomgevingen. In back-ups worden suppress-marks toegepast; definitieve verwijdering volgt automatisch met het reguliere back-upretentieschema.

12.4 Verwijderingsverklaring. Binnen 30 dagen na productieverwijdering verstrekt Verwerker een schriftelijke deletion certificate (datum, systemen, reikwijdte, back-upcyclus, uitzonderingen indien wettelijk vereist).

12.5 Uitzonderingen. Gegevens die Verwerker wettelijk moet bewaren, worden uitsluitend bewaard voor die wettelijke termijn en doel, afgeschermd en niet voor andere doeleinden gebruikt.

12.6 Exit-support. Verwerker verleent redelijke technische assistentie bij migratie (uitleg datamodel, API-endpoints, mapping). Tot 30 dagen na beëindiging geldt dit kosteloos voor basisvragen; uitgebreide ondersteuning (bijv. dataconversies, script-ontwikkeling) is tegen vooraf geoffreerde tarieven.

12.7 Continuïteit en escrow (optioneel). Indien Partijen dit afspreken, kan broncode/technische documentatie onder escrow worden geplaatst; voorwaarden (events, releases, kosten) worden vastgelegd in een apart addendum.

12.8 Intellectuele eigendom. Alle intellectuele eigendomsrechten op de Diensten berusten bij Verwerker of zijn licentiegevers. Datagegevens van Verantwoordelijke (inclusief door of namens hem ingevoerde Persoonsgegevens en afgeleide rapportages) blijven eigendom van Verantwoordelijke.

12.9 Overleving. Geheimhouding, aansprakelijkheid, audit van afgesloten periode, en dit artikel 12 blijven na beëindiging van kracht voor zover nodig om verplichtingen af te ronden en rechten te handhaven.

13. Aansprakelijkheid & vrijwaring

13.1 Relatie met hoofdovereenkomst. Aansprakelijkheid is geregeld in de hoofdovereenkomst. Voor verwerkingen onder deze Overeenkomst gelden aanvullingen hieronder. Bij strijdigheid prevaleert dit artikel voor zover het dataprotectie betreft.

13.2 Toerekening. Iedere Partij is aansprakelijk voor (i) eigen schendingen van deze Overeenkomst en de AVG, en (ii) toerekenbare daden/nalatigheden van door haar ingeschakelde (sub)verwerkers of hulppersonen.

13.3 Schadebeperkingen. a) Indirecte schade. Uitsluiting van gevolg-, reputatie-, en winstdervingsschade, behalve voor zover veroorzaakt door opzet of bewuste roekeloosheid van het leidinggevend management. b) Datalek-specifiek. Redelijke en aantoonbare kosten van incidentrespons, forensics en wettelijke meldingen vallen wél onder directe schade indien het incident aan Verwerker of zijn subverwerker toerekenbaar is.

13.4 Aansprakelijkheidsplafond. De totale aansprakelijkheid van Verwerker uit of in verband met deze Overeenkomst is beperkt tot een maximumbedrag van €500.000 (vijfhonderdduizend euro) per verzekeringsjaar, of – indien het verzekerde bedrag onder de van toepassing zijnde bedrijfsaansprakelijkheids- en/of cyberverzekering lager is – tot het daadwerkelijk verzekerde bedrag volgens de polis, met inachtneming van de toepasselijke voorwaarden en uitsluitingen. Uitzonderingen op dit plafond zijn: (i) overlijden of persoonlijk letsel, (ii) opzet of bewuste roekeloosheid, (iii) inbreuk op de in deze Overeenkomst opgenomen geheimhoudingsverplichtingen, en (iv) door een

toezichthouder opgelegde boetes of schadevergoedingen die rechtstreeks het gevolg zijn van een aan Verwerker toerekenbare schending van de AVG (artikel 82 AVG).

13.5 Administratieve boetes. Eventuele door een toezichthouder opgelegde boetes worden gedragen door de Partij aan wie de overtreding is toe te rekenen, met inachtneming van artikel 13.4 voor zover toepasselijk op schadevergoedingen (niet op de boete zelf indien uitsluiting/doorbelasting wettelijk is verboden).

13.6 Vrijwaring door Verwerker. Verwerker vrijwaart Verantwoordelijke tegen redelijke, aantoonbare schade en kosten voortvloeiend uit een derde-claim die stelt dat Verwerker in strijd heeft gehandeld met (i) deze Overeenkomst of (ii) de AVG, voor zover die claim het gevolg is van toerekenbaar handelen van Verwerker of zijn subverwerkers. Voorwaarde is dat Verantwoordelijke (a) Verwerker onverwijld schriftelijk informeert, (b) Verwerker de exclusieve regie geeft over verweer en schikking (redelijk overleg), en (c) alle redelijke medewerking verleent.

13.7 Vrijwaring door Verantwoordelijke. Verantwoordelijke vrijwaart Verwerker voor derde-claims die voortvloeien uit: (i) verwerking op uitdrukkelijke instructie van Verantwoordelijke die in strijd is met toepasselijk recht, of (ii) door Verantwoordelijke aangeleverde gegevens die onrechtmatig zijn verzameld of verstrekt, behoudens zover de schade mede het gevolg is van Verwerkers toerekenbaar handelen.

13.8 Schadelimitatieplicht. Partijen nemen redelijke maatregelen om schade te beperken en te voorkomen (mitigatie).

14. Overige bepalingen, wijzigingen, kennisgevingen & recht/fora

14.1 Wijzigingen (change control). Verwerker mag deze Overeenkomst aanpassen indien dit noodzakelijk is door gewijzigde wet- of regelgeving of assurance-eisen. Dergelijke wijzigingen worden minimaal 30 dagen vooraf gemeld met toelichting. Leidt een wijziging tot minder bescherming of extra kosten, dan overleggen Partijen over een oplossing. Bij uitblijven daarvan mag Verwerkingsverantwoordelijke het betreffende onderdeel zonder boete beëindigen.

14.2 Kennisgevingen. Juridisch relevante kennisgevingen onder deze Overeenkomst (o.a. datalekmeldingen, subverwerkerwijzigingen, doorgiften) worden schriftelijk gedaan aan het door Partijen opgegeven privacy/security-contactpunt. Functionele supportmeldingen verlopen via het reguliere supportkanaal.

14.3 Overdracht & zeggenschapswijziging. Geen van beide Partijen mag haar rechten/verplichtingen onder deze Overeenkomst overdragen zonder voorafgaande schriftelijke toestemming van de andere Partij, behoudens overdracht binnen de groep of in het kader van fusie/overname van nagenoeg alle activa van de overdraaggende Partij, mits (i) de verkrijger gebonden wordt aan gelijkwaardige verplichtingen en (ii) Verantwoordelijke tijdig wordt geïnformeerd.

14.4 Rangorde. De volgende hiërarchie geldt bij tegenstrijdigheden: (1) dit hoofddeel van de Verwerkersovereenkomst, (2) Bijlagen A–D bij deze Overeenkomst, (3) de hoofdovereenkomst incl. SLA's en algemene voorwaarden, uitsluitend voor zover verenigbaar met de AVG.

14.5 Onafhankelijkheid bepalingen. Nietigheid of onafdwingbaarheid van een bepaling laat de geldigheid van de overige bepalingen onverlet. Partijen vervangen de ongeldige bepaling door een geldige bepaling die de strekking het dichtst benadert.

14.6 Geen afstand. Het niet (direct) afdwingen van een recht impliceert geen afstand van dat recht.

14.7 Volledige afspraak. Deze Overeenkomst vormt, tezamen met haar bijlagen, de volledige afspraak tussen Partijen over verwerkingen onder de Diensten en vervangt eerdere (concept)afspraken hierover.

14.8 Toepasselijk recht & forum. Op deze Overeenkomst is Nederlands recht van toepassing. Geschillen worden exclusief voorgelegd aan de bevoegde rechter in het arrondissement Overijssel, locatie Almelo (tenzij dwingendrechtelijk anders voorgeschreven).

14.9 Taal. Deze Overeenkomst is opgesteld in het Nederlands. Vertalingen dienen uitsluitend ter informatie; bij interpretatieverschillen prevaleert de Nederlandse tekst. Bijlage A — Verwerkingsdetails (scope & AI-kaders) A1. Modules & doeleinden • Matching & scoring (AI-ondersteund): skill-based voorselectie op basis van cv/ervaring vs. vacatureprofiel. • Kandidaatbeheer: statusupdates, notities, taken, planning. • Communicatie: interviewplanning, e-mail/sjablonen, notificaties. • Rapportage & kwaliteitsverbetering: funnels, time-to-hire, conversies, model-evaluaties. • Support & security: foutanalyse, incidentafhandeling, misbruikdetectie. A2. Verwerkingen (per module, kernhandelingen) • Matching: inname → normalisatie → feature-extractie → (pseudoniem) scoreberekening → presentatie. • Beheer: aanmaken/bewerken records, rollen/rechten, export op instructie. • Communicatie: versturen/ontvangen, logging van bezorgstatus (geen inhoudsanalyse buiten support). • Rapportage: aggregaties, geen hergebruik voor andere klanten/algemene verbetering zonder instructie. • Support: tijdelijk, doelgebonden inzien van relevante records/logs. A3. Categorieën betrokkenen • Sollicitanten/kandidaten; interne gebruikers bij Verantwoordelijke (recruiters/hiring managers); optioneel referenten. A4. Categorieën persoonsgegevens (voorbeeldlijst, configureerbaar) • Identiteit & contact: naam, e-mail, telefoon, woonplaats. • Professioneel: opleiding, werkervaring, certificaten, vaardigheden, beschikbaarheid, portfolio-links. • Matchingdata: modelinputs (skills/ervaring), scores, tags, feedback. • Technisch: account-ID, tijdstempels, IP, user agent, auditlogs. • Beeld/ documenten (optioneel): cv-bestanden, profielfoto's (indien aangeleverd). Bijzonder: niet beoogd. Vrije tekstvelden beperken/configureren. A5. Rechtsgrond & informatieplicht • Verantwoordelijke bepaalt per doel de rechtsgrond en informeert betrokkenen. Verwerker ondersteunt (exporten, verwijdering) conform art. 9. A6. Locaties & doorgiften • Primair binnen EU/EER. Eventuele support-toegang van buiten EER valt onder art. 6 (SCC + TIA) en wordt gespecificeerd in

Bijlage C. A7. Retentie (samenvatting; detail in Bijlage B) • Kandidaten: 12 mnd na laatste activiteit → anonimiseer/verwijder. • Logs: app 180 dagen; security 12 mnd. • Back-ups: rolling (bijv. 35 dagen). • Exports: 14 dagen. A8. AI-specifieke kaders • Datasets: uitsluitend dataminimale, gedocumenteerde features. • Geen training/fine-tuning op herleidbare persoonsgegevens zonder schriftelijke instructie + passende waarborgen. • Bias & kwaliteit: pre-release fairness-checks; modelkaart met doel/inputs/metrics; drift-monitoring. • Explainability: op verzoek managementsamenvatting van logische onderdelen van het scoringproces. • Verboden: re-identificatie; cross-tenant training; algemeen modelgebruik buiten overeengekomen doelen. A9. DPIA-triggers (indicatief)
•Grootschalige/geautomatiseerde profilering met rechtsgevolg (niet beoogd). • Gebruik van bijzondere categorieën (niet beoogd). • Systematische monitoring van publiek toegankelijke ruimtes (n.v.t.). → Indien toch aan de orde: Verantwoordelijke initieert DPIA; Verwerker levert technische input. Bijlage B — Beveiligingsmaatregelen & Retentie (operationeel) B1. Toegangsbeheer & identiteiten • RBAC per rol; MFA voor beheer; quarterly access review; JIT-elevatie; individuele accounts (geen shared). B2. Cryptografie & sleutelbeheer • TLS 1.2+ in transit; versleuteling at rest; gescheiden key store; sleutelrotatie. B3. Netwerk/Platform • Gescheiden omgevingen (dev/test/acc/prod); WAF/rate-limits/DDoS; patching per risicoprofiel; hardened images. B4. SDLC & geheimen • Code review, SAST/SCA in CI; periodieke DAST/pen-test; secrets manager; change management met 4-ogen. B5. Logging/monitoring • Centrale, immutabele logs; detectie op aanmeld-/export-/privilege-anomalieën; 24/7 P1-alarming. B6. Dataclassificatie & -segregatie • Classificatiebeleid; tenant-isolatie; testdata geanonimiseerd/synthetisch; AV-scan + filetype/size-limits. B7. Back-up/Herstel & continuïteit • Versleutelde back-ups binnen afgesproken EU-regio's; hersteltests ≥ 2× p/j; RPO/RTO-rapportage. B8. Derden & assurance • Security due diligence; keten-assurance (ISO/SOC-samenvattingen, pen-test samenvattingen). B9. Retentieschema (configureerbaar) • Kandidatenprofiel/cv/matching: 12 mnd na laatste activiteit → anonimiseer of verwijder. • App- & auditlogs: 180 dagen (app); 12 mnd (security). • Supporttickets: 24 mnd na sluiting.

• Back-ups: rolling (bijv. 35 dagen). • Tijdelijke exports: 14 dagen. Afwijkingen: vastleggen per tenant/policy-profiel. B10. Incidentrespons (koppeling) • Zie art. 8 voor meld- en RCA-termijnen; technische playbooks als intern document; resultaten opgenomen in verbeterplan. B11. AI-borging (operationeel) • Modelkaart; fairness-tests; dataset governance (data lineage, feature catalogus); reproduceerbare versies; restricties in code/infra om production PII niet in trainingscorpora te laten vloeien. Bijlage C — Subverwerkers & Doorgiften (register + TIA-samenvatting) Wordt actueel gehouden door Verwerker; wijzigingen via meldprocedure art. 5.1. Voor elke subverwerker is minimaal onderstaand veldenset ingevuld. C1. Registervelden (per subverwerker) • Naam / KvK (indien NL) • Rol (bijv. cloudhosting, e-mailaflevering, observability, pen-test) • Verwerkingsactiviteiten (korte omschrijving) • Verwerkingslocatie(s) (land/regio) • (Evt.) Toegang buiten EER (ja/nee; remote support?) • Rechtsgrond doorgifte (SCC's/adequaatheidsbesluit/geen) • TIA-status (datum, uitkomst, aanvullende maatregelen ja/nee) • Aanvullende maatregelen (bijv. E2EE, pseudonimisering, JIT-access) • Retentie/vernietiging (samenvatting) • Assurance (ISO/SOC; samenvattingsrapport

beschikbaar) C2. Notificatie & bezwaar • Verwerker meldt ≥30 dagen vooraf; Verantwoordelijke kan gemotiveerd bezwaar maken (art. 5.5). • Bij urgentie (continuïteit) verkorte termijn, met zo snel mogelijk volledige info. C3. Remote access • Elke remote toegang van buiten de EER wordt als (potentiële) doorgifte behandeld (SCC + TIA). Tijdgebonden, gelogd, least-privilege. C4. Doorgifte buiten EU/EER (Schrems II) • Conform art. 6: SCC's + TIA + aanvullende maatregelen; opschorting als adequate bescherming niet mogelijk is. C5. AI-specifiek

• Subverwerker met AI-functionaliteit: geen training/fine-tuning op herleidbare PII; uitsluitend geanonimiseerde/aggregaten tenzij expliciet overeengekomen in Bijlage A + passende waarborgen. Voorbeeldregel (te vervangen door jullie werkelijke leveranciers): • ACME Cloud B.V. — Hosting & DB — EU (Frankfurt/Amsterdam) — Geen toegang buiten EER — Assurance: ISO 27001/SOC 2 (samenvatting op verzoek). Bijlage D — Processen & contactpunten D1. Contactpunten • Privacy/AVG (juridisch): dev@kiwiconnect.nl • Security/incidenten (24/7 P1): dev@kiwiconnect.nl • Operationele support: hallo@kiwiconnect.nl (kantoortijden) • D2. Verzoeken van betrokkenen (DSR) • Inkomend kanaal: via Verantwoordelijke; als rechtstreeks bij Verwerker binnen → direct doorzetten naar Verantwoordelijke + ontvangstbevestiging. • Doorlooptijden: zó faciliteren dat 30-dagentermijn haalbaar is (initiële reactie binnen 7 dagen). • Uitvoering: exports (CSV/JSON), rectificaties, wissing/suppress, beperking/opt-out; audittrail per verzoek. D3. Incident/datalek • T0 = detectie; melding binnen 24 uur met kerninformatie; updates tot closure. • RCA binnen 10 werkdagen na containment; verbeterplan met termijnen. D4. Auditverzoeken • Tiered aanpak (documenten → remote → onsite), 1× per 12 mnd, 10 werkdagen vooraf; NDA voor auditoren; keten-assurance voor subverwerkers. D5. Wijzigingen (subverwerkers/doorgiften) • Workflow: aankondiging → bezwaarwindow → (indien nodig) alternatief of beëindiging betreffende onderdeel (pro rata). D6. Exit & data-export • Binnen 30 dagen na einde: 1 volledige export (JSON/CSV + bijlagen) + veldenschema. • Verwijderingsverklaring binnen 30 dagen na productieverwijdering; suppress in back-ups tot einde cyclus.