



Privacy-, Security- en Compliancehandboek

EQObserve - handelsnaam van Onderwijsbekwaam B.V.

Organisatie	Onderwijsbekwaam B.V.
Handelsnaam	EQObserve
Versie	1.0
Status	Definitief concept
Datum	juli 2026
Contact	info@eqobserve.com

Inhoudsopgave

1. Inleiding
2. Privacy- en Security Statement
3. Verwerkersovereenkomst (DPA)
4. Informatiebeveiligingsbeleid
5. Register van Subverwerkers
6. Register van Verwerkingsactiviteiten
7. Data Protection Impact Assessment (DPIA)
8. Incident Response & Datalekprotocol
9. Bewaar- en Vernietigingsbeleid
10. Cookie Statement
11. AI- en Algoritmeverklaring

Hoofdstuk 1

Inleiding

1.1 Over EQObserve

EQObserve is een digitale applicatie die onderwijsprofessionals en onderwijsorganisaties ondersteunt bij het uitvoeren, registreren en analyseren van observaties binnen het onderwijs. De applicatie is ontwikkeld met als doel de professionele ontwikkeling van medewerkers te ondersteunen door middel van gestructureerde observaties en inzichtelijke rapportages.

EQObserve is een handelsnaam van Onderwijsbekwaam B.V.

Onderwijsbekwaam B.V. levert de technische infrastructuur, beheert de applicatie en verwerkt persoonsgegevens uitsluitend ten behoeve van de dienstverlening aan onderwijsinstellingen.

1.2 Doel van dit handboek

Dit Privacy-, Security- en Compliancehandboek beschrijft hoe Onderwijsbekwaam B.V.

persoonsgegevens verwerkt en beveiligt en op welke wijze invulling wordt gegeven aan de wettelijke verplichtingen die voortvloeien uit de Algemene Verordening Gegevensbescherming (AVG).

Het handboek dient tevens als documentatie voor:

- onderwijsinstellingen;
- Functionarissen Gegevensbescherming (FG);
- privacy officers;
- auditors;
- leveranciersbeoordelingen;
- DPIA's;
- aanbestedingen;
- interne kwaliteitsborging.

Het document vormt het centrale beleidsdocument rondom privacy en informatiebeveiliging binnen EQObserve.

1.3 Reikwijdte

Dit handboek is van toepassing op alle persoonsgegevens die door Onderwijsbekwaam B.V. worden verwerkt binnen de EQObserve-applicatie.

Het handboek is van toepassing op:

- webapplicaties;
- mobiele applicaties;
- Single Sign-On (SSO)-koppelingen;
- beheersystemen;
- ondersteunende ICT-infrastructuur;

- ondersteuningsprocessen.

Alle medewerkers, ingehuurde professionals en leveranciers die betrokken zijn bij de dienstverlening dienen dit beleid na te leven.

1.4 Juridisch kader

Onderwijsbekwaam B.V. verwerkt persoonsgegevens overeenkomstig de geldende Europese en Nederlandse wet- en regelgeving.

De dienstverlening is gebaseerd op onder andere:

- Algemene Verordening Gegevensbescherming (EU 2016/679);
- Uitvoeringswet Algemene Verordening Gegevensbescherming;
- relevante bepalingen uit het Burgerlijk Wetboek;
- toepasselijke regelgeving op het gebied van informatiebeveiliging;
- de uitgangspunten van Privacy by Design en Privacy by Default zoals bedoeld in artikel 25 AVG.

Daarnaast volgt Onderwijsbekwaam B.V. de algemeen geaccepteerde beveiligingsprincipes die aansluiten bij normen als ISO/IEC 27001 en de BIO (Baseline Informatiebeveiliging Overheid) voor zover deze passend zijn voor de dienstverlening. Hoewel Onderwijsbekwaam B.V. momenteel niet ISO 27001-gecertificeerd is (tenzij dit in de toekomst verandert), is het informatiebeveiligingsbeleid ingericht volgens de uitgangspunten van deze norm.

1.5 Rollen en verantwoordelijkheden

Binnen de dienstverlening worden de volgende rollen onderscheiden.

Onderwijsinstelling De onderwijsinstelling bepaalt:

- welke medewerkers gebruikmaken van EQObserve;
- voor welke doeleinden observaties plaatsvinden;
- welke gegevens worden ingevoerd;
- wie toegang heeft tot de rapportages.

De onderwijsinstelling is daarmee in beginsel Verwerkingsverantwoordelijke in de zin van de AVG.

Onderwijsbekwaam B.V.

Onderwijsbekwaam B.V. faciliteert de verwerking van persoonsgegevens uitsluitend ten behoeve van de dienstverlening.

Onderwijsbekwaam B.V. treedt daarbij op als Verwerker als bedoeld in artikel 28 AVG.

De verwerking vindt uitsluitend plaats overeenkomstig de afspraken met de onderwijsinstelling.

Gebruikers Gebruikers zijn medewerkers van onderwijsinstellingen die bevoegd zijn gebruik te maken van EQObserve.

Gebruikers zijn verantwoordelijk voor:

- het zorgvuldig omgaan met hun account;
- het juist invoeren van gegevens;
- het vertrouwelijk houden van hun inloggegevens;
- het melden van beveiligingsincidenten.

1.6 Uitgangspunten

Onderwijsbekwaam B.V. hanteert de volgende uitgangspunten bij alle verwerkingen.

Dataminimalisatie Alleen persoonsgegevens die noodzakelijk zijn voor de dienstverlening worden verwerkt.

Doelbinding Persoonsgegevens worden uitsluitend verwerkt voor vooraf vastgestelde en gerechtvaardigde doeleinden.

Opslagbeperking Persoonsgegevens worden niet langer bewaard dan noodzakelijk.

Alle persoonsgegevens worden maximaal één jaar bewaard.

Na afloop van deze termijn worden de gegevens automatisch en onomkeerbaar geanonimiseerd.

Juistheid Gebruikers en onderwijsinstellingen kunnen persoonsgegevens laten corrigeren indien deze onjuist blijken.

Integriteit en vertrouwelijkheid Persoonsgegevens worden beschermd door passende technische en organisatorische beveiligingsmaatregelen.

Transparantie Gebruikers worden duidelijk geïnformeerd over:

- welke gegevens worden verwerkt;
- waarom deze worden verwerkt;
- hoe lang deze worden bewaard;
- welke rechten zij hebben.

Accountability Onderwijsbekwaam B.V. documenteert de genomen privacy- en beveiligingsmaatregelen en kan aantonen dat de verwerking voldoet aan de eisen van de AVG.

1.7 Privacy by Design

Bij de ontwikkeling van EQObserve zijn privacy en informatiebeveiliging vanaf het eerste ontwerp geïntegreerd.

Dit betekent onder meer dat:

- alleen noodzakelijke persoonsgegevens worden verwerkt;
- standaard de meest privacyvriendelijke instellingen worden toegepast;
- persoonsgegevens logisch worden gescheiden van observatiegegevens;
- persoonsgegevens na één jaar automatisch worden geanonimiseerd;
- uitsluitend geanonimiseerde gegevens worden gebruikt voor statistische analyses en kwaliteitsverbetering.

1.8 Informatiebeveiliging

Onderwijsbekwaam B.V. streeft naar een hoog niveau van informatiebeveiliging.

Daarbij wordt uitgegaan van de drie klassieke beveiligingsdoelstellingen:

- **Beschikbaarheid** – gegevens zijn beschikbaar voor bevoegde gebruikers.
- **Integriteit** – gegevens blijven volledig en juist.
- **Vertrouwelijkheid** – uitsluitend bevoegde personen hebben toegang.

Deze uitgangspunten vormen de basis voor alle technische en organisatorische beveiligingsmaatregelen die in dit handboek worden beschreven.

1.9 Contact

Voor vragen over privacy, informatiebeveiliging of de verwerking van persoonsgegevens kan contact worden opgenomen met:

Onderwijsbekwaam B.V.

Handelend onder de naam EQObserve E-mail: info@eqobserve.com

Hoofdstuk 2

Privacy- en Security Statement

2.1 Doel van dit Privacy- en Security Statement

Onderwijsbekwaam B.V., handelend onder de naam EQObserve, hecht grote waarde aan de bescherming van persoonsgegevens en aan de beveiliging van de informatie die aan haar wordt toevertrouwd.

In dit Privacy- en Security Statement wordt uitgelegd:

- welke persoonsgegevens worden verwerkt;
- waarom deze persoonsgegevens worden verwerkt;
- op welke rechtsgrond de verwerking plaatsvindt;
- hoe persoonsgegevens worden beveiligd;
- hoe lang gegevens worden bewaard;
- welke rechten betrokkenen hebben;
- welke verantwoordelijkheden Onderwijsbekwaam B.V. en de onderwijsinstelling hebben.

Dit statement is van toepassing op alle diensten, websites, webapplicaties en mobiele applicaties die door Onderwijsbekwaam B.V. onder de handelsnaam EQObserve worden aangeboden.

2.2 Wie zijn wij?

EQObserve is een handelsnaam van:

Onderwijsbekwaam B.V.

E-mail: info@eqobserve.com Onderwijsbekwaam B.V. ontwikkelt software die onderwijsprofessionals ondersteunt bij observaties, professionele ontwikkeling en kwaliteitsverbetering binnen onderwijsorganisaties.

Afhankelijk van de wijze waarop EQObserve wordt gebruikt, treedt Onderwijsbekwaam B.V.

op als:

- Verwerker in de zin van artikel 28 AVG, wanneer persoonsgegevens worden verwerkt in opdracht van een onderwijsinstelling.
- Verwerkingsverantwoordelijke voor de beperkte persoonsgegevens die noodzakelijk zijn voor de eigen bedrijfsvoering, zoals contactgegevens van klanten, leveranciers en websitebezoekers.

Voor de verwerking van observatiegegevens binnen de applicatie is de onderwijsinstelling in beginsel de verwerkingsverantwoordelijke.

2.3 Onze privacyprincipes

Onderwijsbekwaam B.V. verwerkt persoonsgegevens volgens de volgende uitgangspunten:

- rechtmatigheid;
- behoorlijkheid;
- transparantie;

- doelbinding;
- dataminimalisatie;
- juistheid;
- opslagbeperking;
- integriteit;
- vertrouwelijkheid;
- aantoonbare naleving (accountability).

Deze uitgangspunten vormen de basis van alle processen binnen EQObserve.

2.4 Welke persoonsgegevens verwerken wij?

EQObserve verwerkt uitsluitend persoonsgegevens die noodzakelijk zijn voor het functioneren van de applicatie.

De volgende persoonsgegevens kunnen worden verwerkt:

Persoonsgegevens Doel Naam van de medewerker Identificatie binnen de applicatie E-mailadres Authenticatie, communicatie en gebruikersbeheer Onderwijsinstelling Organisatiekoppeling Afdeling Rapportages en organisatorische indeling Leerjaar waaraan wordt Context van observaties lesgegeven Datum van de observatie Planning, rapportage en analyse Deze gegevens kunnen:

- handmatig worden ingevoerd;
- automatisch worden ontvangen via een Single Sign-On (SSO)-koppeling.

Er worden geen andere persoonsgegevens verwerkt tenzij een onderwijsinstelling hier expliciet om verzoekt en hierover aanvullende afspraken worden gemaakt.

2.5 Bijzondere persoonsgegevens

EQObserve verwerkt geen bijzondere persoonsgegevens zoals bedoeld in artikel 9 AVG.

De applicatie is niet bedoeld voor het verwerken van gegevens over:

- gezondheid;
- ras of etnische afkomst;
- religie;
- politieke overtuigingen;
- seksuele geaardheid;
- biometrische gegevens;
- genetische gegevens;
- strafrechtelijke gegevens.

Gebruikers dienen dergelijke gegevens ook niet op te nemen in observaties of vrije tekstvelden.

2.6 Doeleinden van de verwerking

Persoonsgegevens worden uitsluitend verwerkt voor de volgende doeleinden:

Gebruikersbeheer Het aanmaken, beheren en verwijderen van gebruikersaccounts.

Authenticatie Het mogelijk maken van veilige toegang via gebruikersnaam, wachtwoord of Single Sign-On.

Uitvoeren van observaties Het koppelen van observaties aan de juiste medewerker.

Rapportages Het beschikbaar stellen van observaties aan bevoegde gebruikers.

Ondersteuning Het verlenen van technische ondersteuning en gebruikerssupport.

Beveiliging Het beschermen van de applicatie tegen onbevoegde toegang en misbruik.

Kwaliteitsverbetering Na anonimisering worden observatiegegevens gebruikt voor statistische analyses, benchmarking en het verbeteren van de dienstverlening.

Persoonsgegevens worden niet gebruikt voor:

- commerciële profilering;
- advertenties;
- verkoop aan derden;
- geautomatiseerde besluitvorming;
- het trainen van generatieve AI-modellen.

2.7 Rechtsgrondslag

De verwerking vindt plaats op basis van artikel 6 AVG.

Afhankelijk van de situatie zijn de volgende grondslagen van toepassing.

Uitvoering van een overeenkomst Voor het leveren van de EQObserve-dienstverlening.

Wettelijke verplichting Voor zover wettelijke verplichtingen daartoe aanleiding geven.

Gerechtvaardigd belang Voor:

- informatiebeveiliging;
- systeembeheer;
- fraudepreventie;
- kwaliteitsverbetering;
- het uitvoeren van statistische analyses op volledig geanonimiseerde gegevens.

Wanneer persoonsgegevens niet langer noodzakelijk zijn, worden deze geanonimiseerd.

2.8 Single Sign-On (SSO)

Wanneer een onderwijsinstelling gebruikmaakt van Single Sign-On ontvangt EQObserve uitsluitend de gegevens die noodzakelijk zijn voor authenticatie en gebruikersbeheer.

Afhankelijk van de inrichting van de Identity Provider kunnen de volgende attributen worden ontvangen:

- naam;
- e-mailadres;
- onderwijsinstelling;
- afdeling;
- leerjaar.

EQObserve verwerkt uitsluitend de gegevens die noodzakelijk zijn voor de dienstverlening.

2.9 Bewaartermijnen

Onderwijsbekwaam B.V. hanteert het uitgangspunt dat persoonsgegevens niet langer worden bewaard dan noodzakelijk.

De bewaartermijnen zijn als volgt.

Gegevens Bewaartermijn Persoonsgegevens maximaal 1 jaar Geanonimiseerde onbeperkt observatiegegevens
Na afloop van één jaar worden alle persoonsgegevens automatisch en onomkeerbaar geanonimiseerd.

Na anonimisering zijn de gegevens niet langer tot een natuurlijke persoon herleidbaar.

Deze gegevens worden uitsluitend gebruikt voor:

- trendanalyses;
- benchmarking;
- kwaliteitsverbetering;
- wetenschappelijke en statistische analyses.

2.10 Verwerking binnen Europa

Alle persoonsgegevens worden uitsluitend verwerkt binnen de Europese Economische Ruimte (EER).

Onderwijsbekwaam B.V. maakt gebruik van de Europese hostingdiensten van STRATO.

Persoonsgegevens worden niet opgeslagen of verwerkt buiten de EER.

Indien toekomstige dienstverlening verwerking buiten de EER noodzakelijk maakt, zal dit uitsluitend plaatsvinden indien wordt voldaan aan Hoofdstuk V van de AVG en passende waarborgen zijn getroffen.

2.11 Beveiliging

Onderwijsbekwaam B.V. treft passende technische en organisatorische maatregelen om persoonsgegevens te beschermen tegen verlies, onbevoegde toegang, vernietiging, wijziging of openbaarmaking.

Onze beveiligingsmaatregelen omvatten onder andere:

Organisatorische maatregelen

- Privacy by Design.
- Privacy by Default.
- Geheimhoudingsplicht voor medewerkers.
- Need-to-know autorisaties.
- Periodieke evaluatie van beveiligingsmaatregelen.
- Procedure voor datalekken.
- Beleid voor toegangsbeheer.

Technische maatregelen

- versleutelde communicatie via TLS;
- beveiligde hosting;
- rolgebaseerde autorisaties;
- logging van beheerdersactiviteiten;
- firewallbescherming;
- periodieke software-updates;
- kwetsbaarhedenbeheer;
- back-ups;

- monitoring van beveiligingsincidenten.

Onderwijsbekwaam B.V. blijft de beveiligingsmaatregelen evalueren en aanpassen aan nieuwe technologische ontwikkelingen en veranderende risico's.

2.12 Verstrekking aan derden

Onderwijsbekwaam B.V. verkoopt geen persoonsgegevens.

Persoonsgegevens worden uitsluitend verstrekt aan:

- de betreffende onderwijsinstelling;
- zorgvuldig geselecteerde subverwerkers;
- bevoegde autoriteiten indien een wettelijke verplichting daartoe bestaat.

Met iedere subverwerker wordt een verwerkersovereenkomst gesloten.

2.13 Rechten van betrokkenen

Betrokkenen hebben, voor zover de AVG daarop van toepassing is, recht op:

- inzage;
- rectificatie;
- verwijdering;
- beperking van verwerking;
- overdraagbaarheid van gegevens;
- bezwaar tegen verwerking.

Verzoeken kunnen worden ingediend via:

info@eqobserve.com Onderwijsbekwaam B.V. zal dergelijke verzoeken, indien zij optreedt als verwerker, onverwijld doorgeleiden naar de betreffende onderwijsinstelling en waar nodig ondersteuning bieden bij de afhandeling.

2.14 Datalekken

Onderwijsbekwaam B.V. beschikt over een intern datalekprotocol.

Bij een beveiligingsincident wordt:

1. het incident geregistreerd;
2. de impact beoordeeld;
3. de onderwijsinstelling zonder onnodige vertraging geïnformeerd indien sprake is van een (mogelijk) datalek;
4. ondersteuning geboden bij eventuele meldingen aan de Autoriteit Persoonsgegevens en betrokkenen.

Alle beveiligingsincidenten worden geëvalueerd om herhaling te voorkomen.

2.15 Gebruik van geanonimiseerde gegevens

Na afloop van de bewaartermijn worden persoonsgegevens volledig en onomkeerbaar geanonimiseerd.

De resterende gegevens zijn niet langer herleidbaar tot individuele personen en vallen daardoor niet meer onder de AVG.

Deze geanonimiseerde gegevens worden gebruikt voor:

- het analyseren van trends in onderwijsobservaties;

- benchmarking tussen groepen op geaggregeerd niveau;
- het verbeteren van de observatiemethodiek;
- kwaliteitsverbetering van de applicatie;
- statistische analyses en rapportages.

Onderwijsbekwaam B.V. zal geanonimiseerde gegevens nooit opnieuw proberen te herleiden tot individuele personen.

2.16 Wijzigingen van dit statement

Onderwijsbekwaam B.V. behoudt zich het recht voor dit Privacy- en Security Statement aan te passen wanneer wijzigingen in wetgeving, rechtspraak, technische ontwikkelingen of de dienstverlening daartoe aanleiding geven.

De meest actuele versie is steeds beschikbaar via de website en/of de applicatie van EQObserve.

2.17 Contact en klachten

Voor vragen over privacy, informatiebeveiliging of de verwerking van persoonsgegevens kunt u contact opnemen met:

Onderwijsbekwaam B.V.

Handelend onder de naam EQObserve E-mail: info@eqobserve.com Indien u van mening bent dat uw persoonsgegevens in strijd met de AVG worden verwerkt, heeft u het recht een klacht in te dienen bij de bevoegde toezichthoudende autoriteit, waaronder in Nederland de Autoriteit Persoonsgegevens.

Hoofdstuk 3

Verwerkersovereenkomst (DPA)

3.1 Inleiding

Deze Verwerkersovereenkomst ("Overeenkomst") is opgesteld conform artikel 28 van de Algemene Verordening Gegevensbescherming (AVG) en maakt integraal onderdeel uit van de dienstverlening van Onderwijsbekwaam B.V., handelend onder de naam EQObserve.

Deze overeenkomst regelt de verwerking van persoonsgegevens die Onderwijsbekwaam B.V. namens een onderwijsinstelling uitvoert binnen de EQObserve-applicatie.

Voor zover deze overeenkomst afwijkt van een afzonderlijk gesloten verwerkersovereenkomst tussen partijen, prevaleert de afzonderlijk ondertekende overeenkomst.

3.2 Partijen Verwerkingsverantwoordelijke

De onderwijsinstelling die gebruikmaakt van EQObserve.

Hierna te noemen:

"Verwerkingsverantwoordelijke".

Verwerker Onderwijsbekwaam B.V.

Handelend onder de naam:

EQObserve E-mailadres:

info@eqobserve.com Hierna te noemen:

"Verwerker".

3.3 Definities In deze overeenkomst wordt verstaan onder:

AVG De Algemene Verordening Gegevensbescherming (EU) 2016/679.

Betrokkene De natuurlijke persoon op wie persoonsgegevens betrekking hebben.

Persoonsgegevens Alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon zoals bedoeld in artikel 4 AVG.

Verwerking Elke bewerking met betrekking tot persoonsgegevens zoals omschreven in artikel 4 AVG.

Datalek Een inbreuk in verband met persoonsgegevens zoals bedoeld in artikel 4 lid 12 AVG.

Subverwerker Een derde partij die namens Verwerker persoonsgegevens verwerkt.

3.4 Doel van de verwerking

Verwerker verwerkt persoonsgegevens uitsluitend ten behoeve van de dienstverlening rondom EQObserve.

De verwerking omvat uitsluitend:

- authenticatie;
- gebruikersbeheer;

- registratie van observaties;
- beschikbaar stellen van rapportages;
- technische ondersteuning;
- onderhoud van de applicatie;
- informatiebeveiliging.

Verwerker verwerkt persoonsgegevens uitsluitend overeenkomstig de schriftelijke of elektronische instructies van Verwerkingsverantwoordelijke.

3.5 Categorieën betrokkenen

Deze overeenkomst heeft betrekking op persoonsgegevens van:

- docenten;
- onderwijsassistenten;
- intern begeleiders;
- teamleiders;
- schoolleiders;
- overige medewerkers die gebruikmaken van EQObserve.

3.6 Categorieën persoonsgegevens

Binnen EQObserve worden uitsluitend de volgende persoonsgegevens verwerkt:

Persoonsgegeven Verwerkingsdoel Naam Identificatie gebruiker E-mailadres Authenticatie en communicatie Onderwijsinstelling Organisatiekoppeling Afdeling Rapportages Leerjaar Context observatie Datum observatie Rapportage en planning Verwerker verwerkt geen bijzondere persoonsgegevens als bedoeld in artikel 9 AVG.

Verwerker verwerkt evenmin persoonsgegevens van strafrechtelijke aard.

3.7 Verwerkingsinstructies Verwerker verwerkt persoonsgegevens uitsluitend:

- volgens deze overeenkomst;
- volgens de overeenkomst tussen partijen;
- volgens schriftelijke instructies van Verwerkingsverantwoordelijke;
- overeenkomstig de AVG.

Verwerker zal persoonsgegevens nooit gebruiken voor:

- commerciële doeleinden;
- advertenties;
- profilering;
- verkoop aan derden;
- eigen marketingdoeleinden.

Geanonimiseerde gegevens mogen uitsluitend worden gebruikt overeenkomstig hoofdstuk 2 van dit handboek.

3.7a Verwerking uitsluitend op gedocumenteerde instructies Verwerker verwerkt persoonsgegevens uitsluitend op basis van de gedocumenteerde instructies van Verwerkingsverantwoordelijke, tenzij een op Verwerker rustende wettelijke verplichting tot verwerking bestaat. In dat geval stelt Verwerker Verwerkingsverantwoordelijke

voorafgaand aan de verwerking hiervan op de hoogte, tenzij die wettelijke verplichting deze kennisgeving verbiedt om gewichtige redenen van algemeen belang.

Indien Verwerker van oordeel is dat een instructie in strijd is met de AVG of andere toepasselijke wet- en regelgeving inzake gegevensbescherming, zal Verwerker Verwerkingsverantwoordelijke daarvan onverwijld in kennis stellen.

3.8 Geheimhouding

Alle personen die namens Verwerker toegang hebben tot persoonsgegevens zijn contractueel of wettelijk verplicht tot geheimhouding.

Deze geheimhoudingsplicht blijft ook na beëindiging van de werkzaamheden van kracht.

3.9 Beveiliging

Verwerker treft passende technische en organisatorische beveiligingsmaatregelen overeenkomstig artikel 32 AVG.

Hieronder vallen onder andere:

Organisatorisch

- Privacy by Design;
- Privacy by Default;
- autorisatiebeleid;
- geheimhoudingsbeleid;
- toegangsbeheer;
- incidentmanagement;
- periodieke evaluaties.

Technisch

- TLS-versleuteling;
- beveiligde hosting;
- firewallbescherming;
- logging;
- monitoring;
- back-ups;
- software-updates;
- vulnerability management;
- rolgebaseerde autorisaties.

Deze maatregelen worden periodiek geëvalueerd.

3.9a Vertrouwelijkheid van personen die persoonsgegevens verwerken Verwerker waarborgt dat iedere persoon die onder zijn gezag persoonsgegevens verwerkt:

- uitsluitend toegang heeft tot persoonsgegevens voor zover dit noodzakelijk is voor de uitvoering van zijn werkzaamheden;
- contractueel of wettelijk is gehouden tot geheimhouding;

- passende instructies heeft ontvangen over de bescherming van persoonsgegevens;
- periodiek wordt geïnformeerd over relevante privacy- en informatiebeveiligingsverplichtingen.

Verwerker ziet erop toe dat deze verplichtingen gedurende de gehele periode van toegang tot persoonsgegevens van kracht blijven.

3.10 Hosting

Alle persoonsgegevens worden uitsluitend verwerkt binnen de Europese Economische Ruimte (EER).

Verwerker maakt gebruik van de Europese hostingdiensten van STRATO.

Er vindt geen opslag of verwerking plaats buiten de EER.

3.11 Subverwerkers

Verwerker mag uitsluitend gebruikmaken van zorgvuldig geselecteerde subverwerkers.

Op het moment van vaststelling van deze overeenkomst is de volgende subverwerker actief:

Organisatie Dienst STRATO Hosting Wanneer Verwerker voornemens is een nieuwe subverwerker in te schakelen die persoonsgegevens verwerkt, wordt Verwerkingsverantwoordelijke hierover vooraf geïnformeerd. Verwerkingsverantwoordelijke kan binnen een redelijke termijn gemotiveerd bezwaar maken. Bij inzet van een subverwerker draagt Verwerker er zorg voor dat ten minste gelijkwaardige verplichtingen ten aanzien van privacy, beveiliging en vertrouwelijkheid contractueel worden vastgelegd als in deze overeenkomst.

Verwerker blijft volledig verantwoordelijk voor de werkzaamheden van haar subverwerkers.

3.11a Kennisgeving van nieuwe subverwerkers Verwerker informeert Verwerkingsverantwoordelijke vooraf over voorgenomen wijzigingen in de inzet van subverwerkers die persoonsgegevens verwerken.

Verwerkingsverantwoordelijke heeft het recht binnen een redelijke termijn gemotiveerd bezwaar te maken tegen de voorgenomen wijziging indien daarvoor zwaarwegende privacy- of informatiebeveiligingsgronden bestaan.

Partijen zullen in dat geval in overleg treden om tot een passende oplossing te komen.

3.12 Internationale doorgifte

Persoonsgegevens worden niet verwerkt buiten de Europese Economische Ruimte.

Indien dit in de toekomst noodzakelijk mocht blijken, zal dit uitsluitend plaatsvinden nadat:

- passende waarborgen zijn getroffen;
- de onderwijsinstelling hierover is geïnformeerd;
- aan Hoofdstuk V van de AVG wordt voldaan.

3.13 Bewaartermijnen

Persoonsgegevens worden maximaal één jaar bewaard.

Na afloop van deze termijn worden alle persoonsgegevens automatisch en onomkeerbaar geanonimiseerd.

Na anonimisering zijn de gegevens niet langer herleidbaar tot natuurlijke personen.

Alleen deze geanonimiseerde gegevens worden vervolgens gebruikt voor:

- statistische analyses;
- kwaliteitsverbetering;
- benchmarking;

- trendonderzoek.

3.14 Bijstand aan Verwerkingsverantwoordelijke

Verwerker ondersteunt Verwerkingsverantwoordelijke, voor zover redelijkerwijs mogelijk, bij het voldoen aan diens verplichtingen op grond van de AVG.

Hieronder valt ondersteuning bij:

- verzoeken om inzage;
- correctieverzoeken;
- verwijderingsverzoeken;
- bezwaar tegen verwerking;
- dataportabiliteit;
- DPIA's, indien de door Verwerker uitgevoerde verwerking daarvoor relevante informatie bevat;
- overleg met de Autoriteit Persoonsgegevens, voor zover betrekking hebbend op de dienstverlening van Verwerker.

3.14a Bijstand bij naleving van de AVG Verwerker verleent Verwerkingsverantwoordelijke, rekening houdend met de aard van de verwerking en de beschikbare informatie, redelijke ondersteuning bij het voldoen aan diens verplichtingen op grond van de artikelen 32 tot en met 36 AVG.

Deze ondersteuning omvat, voor zover van toepassing:

- het treffen en evalueren van passende beveiligingsmaatregelen;
- het uitvoeren of actualiseren van een Data Protection Impact Assessment (DPIA);
- overleg met de Autoriteit Persoonsgegevens indien voorafgaande raadpleging noodzakelijk is;
- het verstrekken van informatie die noodzakelijk is om aan de verantwoordingsplicht van Verwerkingsverantwoordelijke te voldoen.

3.15 Datalekken

Verwerker beschikt over een procedure voor het detecteren, registreren en afhandelen van beveiligingsincidenten.

Indien sprake is van een (vermoedelijke) inbreuk in verband met persoonsgegevens:

- wordt Verwerkingsverantwoordelijke zonder onnodige vertraging geïnformeerd;
- verstrekt Verwerker alle beschikbare informatie die noodzakelijk is voor de beoordeling van de meldplicht;
- werkt Verwerker mee aan het beperken van de gevolgen van het incident;
- ondersteunt Verwerker Verwerkingsverantwoordelijke bij een eventuele melding aan de Autoriteit Persoonsgegevens en betrokkenen.

Verwerker houdt een intern register van beveiligingsincidenten bij.

3.16 Audits en controle

Verwerkingsverantwoordelijke heeft het recht om, maximaal eenmaal per kalenderjaar en na een redelijke aankondiging, de naleving van deze overeenkomst te (laten) controleren.

Een audit wordt uitgevoerd:

- op werkdagen;

- zonder onredelijke verstoring van de bedrijfsvoering van Verwerker;
- met inachtneming van de vertrouwelijkheid van andere klanten en bedrijfsgevoelige informatie.

Indien Verwerker beschikt over een actuele onafhankelijke auditverklaring of certificering (zoals ISO/IEC 27001 of een gelijkwaardige verklaring), kan deze in redelijkheid dienen als alternatief voor een fysieke audit.

De kosten van een audit zijn voor rekening van Verwerkingsverantwoordelijke, tenzij uit de audit blijkt dat Verwerker wezenlijk tekortschiet in de nakoming van deze overeenkomst.

3.16a Informatie ten behoeve van compliance Verwerker stelt Verwerkingsverantwoordelijke alle informatie ter beschikking die redelijkerwijs noodzakelijk is om aan te tonen dat wordt voldaan aan de verplichtingen uit artikel 28 AVG.

Hieronder vallen onder meer:

- een actueel overzicht van subverwerkers;
- een beschrijving van de technische en organisatorische beveiligingsmaatregelen;
- relevante auditrapporten, certificeringen of assuranceverklaringen, voor zover beschikbaar;
- informatie die noodzakelijk is voor audits overeenkomstig artikel 3.16 van deze overeenkomst.

Verwerker werkt in redelijkheid mee aan controles en audits, met inachtneming van de vertrouwelijkheid van bedrijfsgevoelige informatie en de beveiliging van de dienstverlening.

3.17 Beëindiging van de dienstverlening

Na beëindiging van de dienstverlening verwijdt Verwerker de nog aanwezige persoonsgegevens overeenkomstig de overeengekomen bewaartermijnen, tenzij een wettelijke verplichting een langere bewaring voorschrijft.

Reeds geanonimiseerde gegevens mogen worden behouden voor de in dit handboek beschreven statistische en kwaliteitsdoeleinden.

3.17a Teruggave en verwijdering van persoonsgegevens Na beëindiging van de dienstverlening verwijdt Verwerker, naar keuze van Verwerkingsverantwoordelijke, alle nog aanwezige persoonsgegevens of stelt deze aan Verwerkingsverantwoordelijke ter beschikking, tenzij een wettelijke verplichting tot verdere bewaring bestaat.

Na voltooiing van de verwijdering bevestigt Verwerker desgevraagd schriftelijk dat de persoonsgegevens zijn verwijderd of geanonimiseerd overeenkomstig de gemaakte afspraken.

Gegevens die overeenkomstig dit handboek volledig en onomkeerbaar zijn geanonimiseerd, mogen door Verwerker worden behouden voor statistische analyses, kwaliteitsverbetering en trendonderzoek, aangezien deze gegevens niet langer als persoonsgegevens in de zin van de AVG kwalificeren.

3.18 Aansprakelijkheid

Iedere partij is verantwoordelijk voor de naleving van de op haar rustende verplichtingen uit de AVG.

Verwerker is uitsluitend aansprakelijk voor schade die het rechtstreekse gevolg is van een toerekenbare tekortkoming in de nakoming van deze overeenkomst of van een handelen of nalaten in strijd met de AVG, voor zover de wet een dergelijke aansprakelijkheid niet uitsluit of beperkt.

Verwerker is niet aansprakelijk voor:

- onjuist of onzorgvuldig gebruik van de applicatie door gebruikers of de onderwijsinstelling;
- onjuiste of onvolledige invoer van gegevens;
- beslissingen die door de onderwijsinstelling of gebruikers worden genomen op basis van rapportages of analyses uit EQObserve;

- schade die ontstaat doordat Verwerkingsverantwoordelijke zijn eigen verplichtingen uit hoofde van de AVG niet naleeft.

Iedere aansprakelijkheid voor indirecte schade, waaronder gevolgschade, gederfde winst, gemiste besparingen, reputatieschade of bedrijfsstagnatie, is uitgesloten, tenzij dwingendrechtelijke bepalingen zich daartegen verzetten.

Niets in deze overeenkomst beperkt de aansprakelijkheid voor schade veroorzaakt door opzet of bewuste roekeloosheid van Verwerker of voor aansprakelijkheid die op grond van dwingend recht niet kan worden uitgesloten.

3.19 Vertrouwelijkheid

Alle informatie die partijen in het kader van deze overeenkomst ontvangen en die redelijkerwijs als vertrouwelijk kan worden aangemerkt, wordt vertrouwelijk behandeld.

Deze verplichting blijft ook na beëindiging van de overeenkomst van kracht.

3.20 Toepasselijk recht en bevoegde rechter

Op deze Verwerkersovereenkomst is uitsluitend Nederlands recht van toepassing.

Geschillen die voortvloeien uit deze overeenkomst worden voorgelegd aan de bevoegde rechter in Nederland, tenzij dwingendrechtelijke bepalingen anders voorschrijven.

3.21 Slotbepalingen

Indien een bepaling uit deze overeenkomst nietig blijkt te zijn of wordt vernietigd, blijven de overige bepalingen onverminderd van kracht. Partijen zullen de betreffende bepaling vervangen door een rechtsgeldige bepaling die zoveel mogelijk aansluit bij het doel en de strekking van de oorspronkelijke bepaling.

Deze Verwerkersovereenkomst vormt samen met de dienstverleningsovereenkomst en dit Privacy-, Security- en Compliancehandboek de volledige afspraken tussen Verwerkingsverantwoordelijke en Verwerker over de verwerking van persoonsgegevens binnen EQObserve.

Hoofdstuk 4

Informatiebeveiligingsbeleid

4.1 Doelstelling

Onderwijsbekwaam B.V., handelend onder de naam EQObserve, beschouwt informatiebeveiliging als een essentieel onderdeel van haar dienstverlening.

Onderwijsinstellingen vertrouwen persoonsgegevens en observatiegegevens toe aan EQObserve. Daarom streeft Onderwijsbekwaam B.V. naar een passend niveau van informatiebeveiliging dat aansluit bij de aard van de dienstverlening, de risico's van de verwerkte gegevens en de eisen van de Algemene Verordening Gegevensbescherming (AVG).

Dit informatiebeveiligingsbeleid beschrijft de uitgangspunten, verantwoordelijkheden en maatregelen die zijn getroffen om persoonsgegevens en bedrijfsinformatie te beschermen tegen ongeautoriseerde toegang, verlies, wijziging of vernietiging.

4.2 Doelstellingen van informatiebeveiliging

Het informatiebeveiligingsbeleid heeft de volgende doelstellingen:

- bescherming van persoonsgegevens;
- bescherming van vertrouwelijke bedrijfsinformatie;
- waarborging van de continuïteit van de dienstverlening;
- voorkomen van datalekken;
- voldoen aan de AVG;
- voldoen aan contractuele verplichtingen richting onderwijsinstellingen;
- minimaliseren van operationele risico's.

Alle beveiligingsmaatregelen zijn erop gericht een evenwicht te vinden tussen gebruiksgemak, betrouwbaarheid en veiligheid.

4.3 Uitgangspunten

Onderwijsbekwaam B.V. baseert haar informatiebeveiligingsbeleid op de volgende uitgangspunten:

Vertrouwelijkheid Informatie is uitsluitend toegankelijk voor personen die daarvoor bevoegd zijn.

Integriteit Gegevens zijn volledig, juist en beschermd tegen ongeautoriseerde wijziging.

Beschikbaarheid Gegevens en systemen zijn beschikbaar wanneer geautoriseerde gebruikers deze nodig hebben.

Privacy by Design Bij de ontwikkeling van nieuwe functionaliteiten worden privacy en beveiliging vanaf het ontwerp meegenomen.

Privacy by Default De standaardinstellingen van EQObserve zijn zo privacyvriendelijk mogelijk ingericht.

Dataminimalisatie Er worden uitsluitend persoonsgegevens verwerkt die noodzakelijk zijn voor de dienstverlening.

Least Privilege Gebruikers ontvangen uitsluitend toegang tot gegevens die noodzakelijk zijn voor hun werkzaamheden.

4.4 Governance

De directie van Onderwijsbekwaam B.V. is eindverantwoordelijk voor het informatiebeveiligingsbeleid.

De directie is verantwoordelijk voor:

- het vaststellen van dit beleid;
- periodieke evaluatie;
- beschikbaar stellen van voldoende middelen;
- naleving van wet- en regelgeving.

Alle medewerkers zijn verantwoordelijk voor zorgvuldig omgaan met informatie en het naleven van dit beleid.

4.5 Risicomanagement

Onderwijsbekwaam B.V. hanteert een risicogebaseerde benadering.

Nieuwe risico's worden periodiek beoordeeld op:

- kans;
- impact;
- beheersbaarheid.

Bij wijzigingen aan de applicatie wordt beoordeeld of aanvullende beveiligingsmaatregelen noodzakelijk zijn.

4.6 Classificatie van informatie

Onderwijsbekwaam B.V. onderscheidt vier classificatieniveaus.

Classificatie Voorbeelden Openbaar Website-informatie Intern Handleidingen, interne documentatie Vertrouwelijk Klantgegevens, gebruikersgegevens Zeer vertrouwelijk Persoonsgegevens, observatiegegevens, authenticatiegegevens Voor iedere classificatie gelden passende beveiligingsmaatregelen.

4.7 Persoonsgegevens

Binnen EQObserve worden uitsluitend de volgende persoonsgegevens verwerkt:

- naam;
- e-mailadres;
- onderwijsinstelling;
- afdeling;
- leerjaar;
- datum van observatie.

Er worden geen bijzondere persoonsgegevens verwerkt.

Na één jaar worden alle persoonsgegevens automatisch en onomkeerbaar geanonimiseerd.

4.8 Toegangsbeheer

Toegang tot persoonsgegevens wordt uitsluitend verleend aan geautoriseerde gebruikers.

Het toegangsbeheer is gebaseerd op de volgende principes:

- individuele accounts;
- unieke gebruikersidentificatie;
- rolgebaseerde autorisaties;
- need-to-know;
- least privilege.

Accounts worden verwijderd zodra een gebruiker geen toegang meer behoort te hebben.

4.9 Authenticatie Gebruikers kunnen zich authenticeren via:

- gebruikersaccount;
- Single Sign-On (SSO), indien de onderwijsinstelling hiervan gebruikmaakt.

Wanneer SSO wordt toegepast, worden uitsluitend de noodzakelijke attributen verwerkt.

Beheeraccounts worden extra beschermd door sterke authenticatie. Waar technisch mogelijk wordt multi-factor authenticatie (MFA) toegepast voor beheerders.

4.10 Wachtwoorden

Wanneer gebruik wordt gemaakt van lokale accounts gelden ten minste de volgende uitgangspunten:

- sterke wachtwoorden;
- veilige opslag van wachtwoorden (gehasht en gesalt);
- geen opslag van wachtwoorden in leesbare vorm;
- wijziging van standaardwachtwoorden vóór ingebruikname.

Gebruikers zijn verantwoordelijk voor het geheimhouden van hun inloggegevens.

4.11 Logging en monitoring

Onderwijsbekwaam B.V. registreert beveiligingsrelevante gebeurtenissen voor zover noodzakelijk voor:

- beveiliging;
- foutanalyse;
- incidentonderzoek;
- continuïteit.

Logging bevat uitsluitend gegevens die noodzakelijk zijn voor deze doeleinden.

Logbestanden worden adequaat beveiligd tegen wijziging of ongeautoriseerde inzage.

4.12 Netwerkbeveiliging

De infrastructuur van EQObserve is beveiligd door middel van passende netwerkmaatregelen.

Hieronder vallen onder meer:

- firewallbescherming;
- versleutelde netwerkverbindingen (TLS);
- beveiligde beheerverbindingen;
- beperking van externe toegang.

4.13 Hosting

Alle gegevens worden opgeslagen binnen de Europese Economische Ruimte.

Onderwijsbekwaam B.V. maakt gebruik van de professionele hostingdiensten van STRATO.

De hostingomgeving voldoet aan algemeen aanvaarde beveiligingsstandaarden voor datacenters.

Er vindt geen verwerking buiten de EER plaats.

4.14 Encryptie

Alle communicatie tussen gebruikers en de applicatie vindt plaats via versleutelde verbindingen.

Waar passend worden gegevens tevens versleuteld opgeslagen.

Onderwijsbekwaam B.V. past actuele cryptografische standaarden toe.

4.15 Softwareontwikkeling

Nieuwe functionaliteiten worden ontwikkeld volgens veilige ontwikkelprincipes.

Hieronder vallen onder meer:

- beveiligingsreviews;
- testen voorafgaand aan productie;
- foutcorrecties;
- periodieke updates;
- aandacht voor bekende kwetsbaarheden (zoals opgenomen in de OWASP Top 10).

Wijzigingen worden gecontroleerd voordat deze beschikbaar worden gesteld aan gebruikers.

4.16 Kwetsbaarhedenbeheer

Onderwijsbekwaam B.V. monitort actief bekende kwetsbaarheden in gebruikte softwarecomponenten.

Indien beveiligingsupdates beschikbaar komen, worden deze binnen een redelijke termijn beoordeeld en, afhankelijk van de ernst van het risico, zo spoedig mogelijk geïmplementeerd.

Kritieke beveiligingsproblemen krijgen prioriteit.

4.17 Back-up en herstel

Van de systemen worden periodiek back-ups gemaakt.

Back-ups worden gebruikt voor:

- herstel na storingen;
- calamiteiten;
- continuïteit van dienstverlening.

Back-ups worden beveiligd opgeslagen en zijn uitsluitend toegankelijk voor geautoriseerde beheerders.

De herstelprocedures worden periodiek getest.

4.18 Continuïteit

Onderwijsbekwaam B.V. streeft naar een hoge beschikbaarheid van de dienstverlening.

Bij storingen worden passende maatregelen genomen om de dienstverlening zo spoedig mogelijk te herstellen.

Bij calamiteiten worden de continuïteitsprocedures gevolgd.

4.19 Incidentmanagement

Alle beveiligingsincidenten worden geregistreerd.

Voor ieder incident wordt beoordeeld:

- oorzaak;
- impact;
- noodzakelijke maatregelen;
- meldplicht.

Indien sprake is van een datalek wordt gehandeld overeenkomstig Hoofdstuk 8 van dit handboek.

4.20 Leveranciersbeheer

Leveranciers die persoonsgegevens verwerken worden vooraf beoordeeld op betrouwbaarheid en beveiliging.

Met iedere subverwerker wordt een overeenkomst gesloten waarin ten minste wordt vastgelegd:

- geheimhouding;
- beveiligingsmaatregelen;
- naleving van de AVG;
- verantwoordelijkheden.

Op dit moment maakt Onderwijsbekwaam B.V. voor de hosting van EQObserve gebruik van STRATO als subverwerker.

4.21 Bewaarbeleid

Persoonsgegevens worden maximaal één jaar bewaard.

Na afloop van deze termijn worden alle persoonsgegevens automatisch en onomkeerbaar geanonimiseerd.

Geanonimiseerde gegevens worden uitsluitend gebruikt voor:

- statistiek;
- trendanalyse;
- benchmarking;
- kwaliteitsverbetering.

4.22 Bewustwording

Onderwijsbekwaam B.V. bevordert beveiligingsbewustzijn binnen de organisatie.

Medewerkers worden geïnformeerd over:

- vertrouwelijkheid;
- omgang met persoonsgegevens;
- beveiligingsincidenten;
- meldplicht datalekken;
- zorgvuldig gebruik van systemen.

4.23 Controle en evaluatie

Dit informatiebeveiligingsbeleid wordt ten minste jaarlijks geëvalueerd.

Daarnaast vindt een tussentijdse evaluatie plaats wanneer:

- wetgeving wijzigt;
- de dienstverlening wezenlijk verandert;
- zich een ernstig beveiligingsincident voordoet;
- nieuwe technologische risico's ontstaan.

4.24 Naleving

Alle medewerkers en eventuele opdrachtnemers van Onderwijsbekwaam B.V. zijn gehouden dit beleid na te leven.

Afwijkingen van dit beleid worden uitsluitend toegestaan na goedkeuring door de directie en uitsluitend indien de beveiliging en privacy van betrokkenen daardoor niet onevenredig worden aangetast.

4.25 Conformiteit met wet- en regelgeving

Onderwijsbekwaam B.V. heeft dit informatiebeveiligingsbeleid ingericht in overeenstemming met:

- de Algemene Verordening Gegevensbescherming (AVG);
- de Uitvoeringswet AVG (UAVG);
- de beginselen van Privacy by Design en Privacy by Default (artikel 25 AVG);
- de beveiligingseisen van artikel 32 AVG;
- de uitgangspunten van ISO/IEC 27001 voor informatiebeveiligingsmanagement, voor zover passend bij de omvang en aard van de organisatie.

Onderwijsbekwaam B.V. streeft naar continue verbetering van haar informatiebeveiliging door periodieke evaluatie van risico's, beveiligingsmaatregelen en relevante wet- en regelgeving.

Hoofdstuk 5

Register van Subverwerkers

5.1 Doel van dit register

Onderwijsbekwaam B.V., handelend onder de naam EQObserve, maakt uitsluitend gebruik van subverwerkers wanneer dit noodzakelijk is voor het leveren van een veilige, betrouwbare en kwalitatief hoogwaardige dienstverlening.

Dit register geeft een actueel overzicht van de organisaties die in opdracht van Onderwijsbekwaam B.V. persoonsgegevens kunnen verwerken ten behoeve van de dienstverlening aan onderwijsinstellingen.

Het register is opgesteld overeenkomstig artikel 28 AVG en ondersteunt de transparantie richting onderwijsinstellingen, Functionarissen Gegevensbescherming (FG's), auditors en toezichthouders.

5.2 Definitie van een subverwerker

Een subverwerker is een organisatie die in opdracht van Onderwijsbekwaam B.V.

persoonsgegevens verwerkt die door een onderwijsinstelling aan EQObserve zijn toevertrouwd.

Een leverancier wordt uitsluitend als subverwerker aangemerkt indien deze daadwerkelijk toegang kan hebben tot persoonsgegevens of deze namens Onderwijsbekwaam B.V.

verwerkt.

Leveranciers die uitsluitend hardware leveren of geen toegang hebben tot persoonsgegevens worden niet als subverwerker beschouwd.

5.3 Selectie van subverwerkers

Onderwijsbekwaam B.V. selecteert uitsluitend subverwerkers die aantoonbaar passende technische en organisatorische beveiligingsmaatregelen hebben getroffen.

Bij de selectie wordt onder andere gekeken naar:

- betrouwbaarheid van de leverancier;
- informatiebeveiliging;
- continuïteit van dienstverlening;
- naleving van de AVG;
- verwerking binnen de Europese Economische Ruimte (EER);
- contractuele waarborgen.

Voor iedere subverwerker wordt een overeenkomst gesloten waarin ten minste afspraken zijn vastgelegd over:

- geheimhouding;
- beveiligingsmaatregelen;
- ondersteuning bij datalekken;
- bewaartermijnen;

- verwijdering van persoonsgegevens;
- auditmogelijkheden, voor zover passend.

5.4 Overzicht van subverwerkers

Op het moment van vaststelling van dit handboek maakt Onderwijsbekwaam B.V. gebruik van de volgende subverwerker.

Subverwerke Dienst Verwerking Verwerkingslocatie r persoonsgegevens STRATO Hosting van de Ja Europese EQObserve-applicatie, Economische Ruimte database en (EER) infrastructuur Toelichting STRATO verzorgt de hosting van de infrastructuur waarop de EQObserve-applicatie draait.

Persoonsgegevens worden uitsluitend opgeslagen en verwerkt binnen de Europese Economische Ruimte.

Onderwijsbekwaam B.V. heeft met STRATO passende contractuele afspraken gemaakt om de beveiliging en vertrouwelijkheid van persoonsgegevens te waarborgen.

5.5 Verwerking buiten de EER

Onderwijsbekwaam B.V. verwerkt persoonsgegevens uitsluitend binnen de Europese Economische Ruimte.

Er worden geen subverwerkers ingezet die persoonsgegevens buiten de EER verwerken.

Indien in de toekomst een subverwerker buiten de EER zou worden ingezet, zal dit uitsluitend plaatsvinden indien:

- wordt voldaan aan hoofdstuk V van de AVG;
- passende waarborgen zijn getroffen;
- de onderwijsinstelling vooraf wordt geïnformeerd;
- de verwerking contractueel is vastgelegd.

5.6 Wijzigingen in subverwerkers

Onderwijsbekwaam B.V. kan nieuwe subverwerkers inschakelen wanneer dit noodzakelijk is voor de dienstverlening.

Voordat een nieuwe subverwerker persoonsgegevens verwerkt:

- wordt beoordeeld of de leverancier voldoet aan de beveiligingseisen van Onderwijsbekwaam B.V.;
- wordt een verwerkersovereenkomst of gelijkwaardige overeenkomst gesloten;
- wordt de onderwijsinstelling hierover geïnformeerd, indien de overeenkomst met de onderwijsinstelling dat voorschrijft.

Onderwijsinstellingen kunnen gemotiveerd bezwaar maken tegen de inzet van een nieuwe subverwerker wanneer daarvoor zwaarwegende privacy- of beveiligingsredenen bestaan.

5.7 Verantwoordelijkheid van Onderwijsbekwaam B.V.

Hoewel werkzaamheden kunnen worden uitbesteed aan een subverwerker, blijft Onderwijsbekwaam B.V. verantwoordelijk voor de naleving van de verplichtingen die voortvloeien uit de AVG en de met de onderwijsinstelling gesloten verwerkersovereenkomst.

Onderwijsbekwaam B.V. ziet erop toe dat iedere subverwerker:

- uitsluitend persoonsgegevens verwerkt op instructie van Onderwijsbekwaam B.V.;
- passende beveiligingsmaatregelen treft;

- vertrouwelijkheid waarborgt;
- persoonsgegevens niet voor eigen doeleinden gebruikt;
- persoonsgegevens niet langer bewaart dan noodzakelijk.

5.8 Beoordeling van subverwerkers Subverwerkers worden periodiek geëvalueerd.

Bij deze beoordeling wordt onder meer gekeken naar:

- beschikbaarheid van de dienstverlening;
- beveiligingsincidenten;
- naleving van contractuele afspraken;
- wijzigingen in de dienstverlening;
- wijzigingen in wet- en regelgeving.

Indien blijkt dat een subverwerker niet langer voldoet aan de gestelde eisen, zal Onderwijsbekwaam B.V. passende maatregelen treffen. Dit kan onder meer bestaan uit aanvullende afspraken, het treffen van extra beveiligingsmaatregelen of het beëindigen van de samenwerking.

5.9 Registerbeheer

Dit register wordt beheerd door Onderwijsbekwaam B.V. en maakt onderdeel uit van het Privacy-, Security- en Compliancehandboek.

Het register wordt bijgewerkt wanneer:

- een nieuwe subverwerker wordt toegevoegd;
- een bestaande subverwerker vervalst;
- de aard van de dienstverlening wijzigt;
- wet- en regelgeving daartoe aanleiding geeft.

Ten minste eenmaal per jaar wordt gecontroleerd of het register nog actueel is.

5.10 Transparantie richting onderwijsinstellingen

Onderwijsbekwaam B.V. streeft naar volledige transparantie over de inzet van subverwerkers.

Op verzoek van een onderwijsinstelling verstrekt Onderwijsbekwaam B.V.:

- het meest actuele subverwerkersregister;
- een toelichting op de aard van de verwerkingen;
- informatie over de getroffen beveiligingsmaatregelen, voor zover dit geen vertrouwelijke bedrijfsinformatie of de beveiliging van de dienstverlening schaadt.

5.11 Samenvatting

Onderwijsbekwaam B.V. beperkt het gebruik van subverwerkers tot het strikt noodzakelijke.

Op het moment van uitgifte van dit handboek wordt uitsluitend gebruikgemaakt van STRATO voor de hosting van de EQObserve-applicatie en de bijbehorende gegevensopslag binnen de Europese Economische Ruimte.

Iedere uitbreiding van het aantal subverwerkers zal worden beoordeeld aan de hand van de uitgangspunten van de AVG, dit handboek en de contractuele afspraken met de onderwijsinstellingen.

Hoofdstuk 6

Register van Verwerkingsactiviteiten

6.1 Doel van dit register

Dit register van verwerkingsactiviteiten is opgesteld overeenkomstig artikel 30 van de Algemene Verordening Gegevensbescherming (AVG).

Het register beschrijft welke persoonsgegevens binnen EQObserve worden verwerkt, waarom deze worden verwerkt, op welke rechtsgrond de verwerking plaatsvindt, welke beveiligingsmaatregelen zijn getroffen en hoe lang de gegevens worden bewaard.

Hoewel Onderwijsbekwaam B.V. als leverancier van EQObserve in de meeste gevallen optreedt als verwerker, houdt zij dit register bij in het kader van haar verantwoordingsplicht (accountability) en ter ondersteuning van onderwijsinstellingen bij hun eigen register van verwerkingsactiviteiten.

Dit register wordt minimaal eenmaal per jaar geëvalueerd en geactualiseerd wanneer wijzigingen in de dienstverlening daartoe aanleiding geven.

6.2 Verwerkingsverantwoordelijke en verwerker

Verwerkingsverantwoordelijke De onderwijsinstelling die gebruikmaakt van EQObserve bepaalt:

- welke medewerkers gebruikmaken van de applicatie;
- welke observaties worden uitgevoerd;
- voor welke doeleinden de gegevens worden verwerkt.

De onderwijsinstelling is daarom in beginsel de Verwerkingsverantwoordelijke.

Verwerker Onderwijsbekwaam B.V., handelend onder de naam EQObserve, verwerkt persoonsgegevens uitsluitend in opdracht van de onderwijsinstelling.

Contactgegevens Onderwijsbekwaam B.V.

E-mail:

info@eqobserve.com

6.3 Overzicht van verwerkingsactiviteiten Verwerking 1 – Gebruikersbeheer

Doel Het aanmaken, beheren en verwijderen van gebruikersaccounts.

Categorie betrokkenen

- docenten;
- onderwijsassistenten;
- teamleiders;
- schoolleiders;
- overige medewerkers.

Persoonsgegevens

- naam;
- e-mailadres;
- onderwijsinstelling;
- afdeling;
- leerjaar.

Rechtsgrond Uitvoering van de overeenkomst tussen de onderwijsinstelling en Onderwijsbekwaam B.V.

(artikel 6 lid 1 onder b AVG) en, voor de onderwijsinstelling als werkgever, de gerechtvaardigde organisatie van de onderwijsprocessen (artikel 6 lid 1 onder f AVG), voor zover van toepassing.

Ontvangers

- Onderwijsbekwaam B.V.
- geautoriseerde beheerders van de onderwijsinstelling.

Bewaartermijn Maximaal één jaar.

Beveiliging

- rolgebaseerde autorisatie;
- TLS;
- beveiligde hosting;
- logging.

Verwerking 2 – Authenticatie Doel Veilige toegang tot de applicatie.

Persoonsgegevens

- naam;
- e-mailadres.

Herkomst

- gebruikersaccount;
- Single Sign-On.

Rechtsgrond Uitvoering van de overeenkomst.

Ontvangers Geen derden, anders dan de hostingprovider voor de technische verwerking.

Bewaartermijn Maximaal één jaar.

Verwerking 3 – Observatieregistratie Doel Registreren van observaties.

Persoonsgegevens

- naam;
- observatiedatum;
- afdeling;
- leerjaar.

Rechtsgrond Uitvoering van de overeenkomst.

Ontvangers Geautoriseerde gebruikers binnen de onderwijsinstelling.

Bewaartermijn Maximaal één jaar.

Na één jaar worden de gegevens volledig geanonimiseerd.

Verwerking 4 – Rapportages Doel Genereren van rapportages ten behoeve van professionele ontwikkeling.

Persoonsgegevens

- naam;
- afdeling;
- leerjaar;
- observatiedatum.

Rechtsgrond Uitvoering van de overeenkomst.

Ontvangers Geautoriseerde gebruikers van de onderwijsinstelling.

Bewaartermijn Maximaal één jaar.

Verwerking 5 – Support Doel Ondersteuning van gebruikers.

Persoonsgegevens

- naam;
- e-mailadres.

Rechtsgrond Uitvoering van de overeenkomst.

Ontvangers Medewerkers van Onderwijsbekwaam B.V. die belast zijn met ondersteuning.

Bewaartermijn Maximaal één jaar.

Verwerking 6 – Beveiliging Doel Bescherming van systemen.

Mogelijke persoonsgegevens

- gebruikersidentificatie;
- technische loggegevens;
- tijdstip van inloggen.

Rechtsgrond Gerechtvaardigd belang (artikel 6 lid 1 onder f AVG) bij het waarborgen van de veiligheid en continuïteit van de dienstverlening.

Bewaartermijn Niet langer dan noodzakelijk voor beveiligingsdoeleinden, met een richttermijn van maximaal twaalf maanden, tenzij een incident een langere bewaring rechtvaardigt.

Verwerking 7 – Geanonimiseerde analyses Doel

- trendanalyse;
- benchmarking;
- kwaliteitsverbetering;
- statistische analyses.

Persoonsgegevens Geen.

Na afloop van de bewaartermijn worden alle persoonsgegevens volledig en onomkeerbaar geanonimiseerd.

De resterende gegevens zijn niet langer persoonsgegevens in de zin van de AVG.

Rechtsgrond Niet van toepassing, aangezien uitsluitend geanonimiseerde gegevens worden verwerkt.

6.4 Categorieën persoonsgegevens

Binnen EQObserve worden uitsluitend de volgende persoonsgegevens verwerkt:

Gegevenscategori Verwerkt e Naam Ja E-mailadres Ja Onderwijsinstelling Ja Afdeling Ja Leerjaar Ja
Observatiedatum Ja

6.5 Bijzondere persoonsgegevens

Onderwijsbekwaam B.V. verwerkt geen bijzondere persoonsgegevens als bedoeld in artikel 9 AVG.

De applicatie is niet ontworpen voor het verwerken van:

- medische gegevens;
- religieuze overtuigingen;
- politieke voorkeur;
- biometrische gegevens;
- genetische gegevens;
- strafrechtelijke gegevens.

Gebruikers worden geïnstrueerd dergelijke gegevens niet in observaties of vrije tekstvelden op te nemen.

6.6 Ontvangers van persoonsgegevens

Persoonsgegevens kunnen uitsluitend worden verwerkt door:

- geautoriseerde medewerkers van de onderwijsinstelling;
- geautoriseerde medewerkers van Onderwijsbekwaam B.V., voor zover noodzakelijk voor beheer en ondersteuning;
- STRATO als hostingprovider.

Persoonsgegevens worden niet verkocht of verstrekt aan commerciële derden.

6.7 Internationale doorgifte

Alle persoonsgegevens worden verwerkt binnen de Europese Economische Ruimte.

Er vindt geen doorgifte plaats naar landen buiten de EER.

Indien dit in de toekomst noodzakelijk mocht zijn, zal uitsluitend gebruik worden gemaakt van passende waarborgen overeenkomstig hoofdstuk V AVG.

6.8 Bewaartermijnen

Onderwijsbekwaam B.V. hanteert de volgende bewaartermijnen.

Gegevens Bewaartermijn Persoonsgegevens maximaal 1 jaar Geanonimiseerde onbeperkt gegevens Na één jaar worden persoonsgegevens automatisch geanonimiseerd.

De anonimisering is zodanig ingericht dat de gegevens redelijkerwijs niet meer tot een natuurlijke persoon kunnen worden herleid.

6.9 Technische en organisatorische maatregelen

Ter bescherming van persoonsgegevens worden onder meer de volgende maatregelen toegepast:

Organisatorisch

- geheimhoudingsplicht;

- autorisatiebeleid;
- Privacy by Design;
- Privacy by Default;
- periodieke evaluaties.

Technisch

- TLS-encryptie;
- beveiligde hosting;
- logging;
- firewall;
- back-ups;
- software-updates;
- monitoring;
- toegangsbeheer.

Deze maatregelen worden periodiek geëvalueerd en waar nodig aangepast.

6.10 Rechten van betrokkenen

Onderwijsbekwaam B.V. ondersteunt de onderwijsinstelling bij de uitoefening van de rechten van betrokkenen.

Hieronder vallen:

- inzage;
- correctie;
- verwijdering;
- beperking;
- dataportabiliteit;
- bezwaar.

Verzoeken worden doorgeleid naar de onderwijsinstelling indien deze optreedt als verwerkingsverantwoordelijke.

6.11 Verantwoordelijkheden Onderwijsinstelling

De onderwijsinstelling is verantwoordelijk voor:

- de rechtmatigheid van de verwerking;
- het informeren van medewerkers;
- de grondslag voor de verwerking;
- het behandelen van verzoeken van betrokkenen.

Onderwijsbekwaam B.V.

Onderwijsbekwaam B.V. is verantwoordelijk voor:

- een veilige verwerking;
- naleving van de verwerkersovereenkomst;
- passende technische en organisatorische beveiligingsmaatregelen;

- ondersteuning van de onderwijsinstelling bij de naleving van de AVG.

6.12 Beheer van dit register

Dit register wordt beheerd door Onderwijsbekwaam B.V.

Het register wordt bijgewerkt wanneer:

- nieuwe persoonsgegevens worden verwerkt;
- nieuwe functionaliteiten worden ontwikkeld;
- nieuwe subverwerkers worden ingezet;
- wet- en regelgeving verandert.

Ten minste eenmaal per kalenderjaar wordt het register beoordeeld op actualiteit en volledigheid.

Hoofdstuk 7

Data Protection Impact Assessment (DPIA)

7.1 Doel van de DPIA

Deze Data Protection Impact Assessment (DPIA) is opgesteld om de privacyrisico's van de verwerking van persoonsgegevens binnen EQObserve systematisch in kaart te brengen en passende beheersmaatregelen vast te leggen.

De DPIA is gebaseerd op artikel 35 van de Algemene Verordening Gegevensbescherming (AVG).

Op basis van de huidige inrichting van EQObserve concludeert Onderwijsbekwaam B.V. dat de verwerking naar verwachting geen hoog restrisico oplevert voor de rechten en vrijheden van betrokkenen, mits de in dit handboek beschreven technische en organisatorische maatregelen worden gehandhaafd.

Deze DPIA dient als standaardbeoordeling. Onderwijsinstellingen kunnen ervoor kiezen deze als basis te gebruiken voor hun eigen DPIA of privacybeoordeling.

7.2 Beschrijving van de verwerking

EQObserve ondersteunt onderwijsinstellingen bij het uitvoeren van observaties en het inzichtelijk maken van professionele ontwikkeling.

De applicatie verwerkt uitsluitend persoonsgegevens die noodzakelijk zijn voor:

- authenticatie;
- gebruikersbeheer;
- registratie van observaties;
- rapportages;
- ondersteuning van gebruikers.

Na één jaar worden alle persoonsgegevens automatisch en onomkeerbaar geanonimiseerd.

De geanonimiseerde gegevens worden uitsluitend gebruikt voor statistische analyses, trendonderzoek en kwaliteitsverbetering.

7.3 Rollen Verwerkingsverantwoordelijke

De onderwijsinstelling.

De onderwijsinstelling bepaalt:

- welke medewerkers gebruikmaken van EQObserve;
- welke observaties plaatsvinden;
- welke doeleinden worden nagestreefd.

Verwerker Onderwijsbekwaam B.V.

Onderwijsbekwaam B.V. verwerkt persoonsgegevens uitsluitend in opdracht van de onderwijsinstelling.

7.4 Beschrijving van de persoonsgegevens

Binnen EQObserve worden uitsluitend de volgende persoonsgegevens verwerkt.

Gegeven Verwerking Naam Ja E-mailadres Ja Onderwijsinstelling Ja Afdeling Ja Leerjaar Ja Observatiedatum Ja
Er worden geen bijzondere persoonsgegevens verwerkt.

Er worden geen strafrechtelijke gegevens verwerkt.

7.5 Betrokkenen

De verwerking heeft uitsluitend betrekking op medewerkers van onderwijsinstellingen.

Hieronder vallen onder meer:

- docenten;
- onderwijsassistenten;
- teamleiders;
- schoolleiders;
- overige medewerkers.

Er worden geen persoonsgegevens van leerlingen verwerkt.

7.6 Doeleinden

De verwerking dient uitsluitend de volgende doeleinden.

- gebruikersbeheer;
- authenticatie;
- observaties;
- rapportages;
- ondersteuning;
- informatiebeveiliging;
- kwaliteitsverbetering op basis van geanonimiseerde gegevens.

Persoonsgegevens worden niet gebruikt voor:

- marketing;
- advertenties;
- commerciële profilering;
- geautomatiseerde besluitvorming;
- AI-training.

7.7 Rechtsgrond De verwerking is gebaseerd op:

- uitvoering van de overeenkomst;
- gerechtvaardigd belang voor informatiebeveiliging;
- gerechtvaardigd belang voor de verwerking van volledig geanonimiseerde statistische gegevens.

7.8 Noodzaak van de verwerking

Voor iedere verwerking is beoordeeld of deze noodzakelijk is.

Gegeven Noodzakelijk Naam Ja E-mailadres Ja Onderwijsinstelling Ja Afdeling Ja Leerjaar Ja Observatiedatum
Ja Geen van deze gegevens wordt verwerkt zonder aantoonbaar functioneel doel.

7.9 Proportionaliteit De verwerking is proportioneel omdat:

- uitsluitend zes persoonsgegevens worden verwerkt;
- geen bijzondere persoonsgegevens worden verwerkt;
- geen persoonsgegevens van leerlingen worden verwerkt;
- persoonsgegevens maximaal één jaar worden bewaard;
- daarna volledige anonimisering plaatsvindt;
- alleen geanonimiseerde gegevens voor langetermijnanalyses worden gebruikt.

7.10 Gegevensstromen Stap 1

Gebruiker meldt zich aan.

↓ Stap 2 Persoonsgegevens worden handmatig ingevoerd of via SSO ontvangen.

↓ Stap 3 Gebruiker voert observatie uit.

↓ Stap 4 Rapportages worden beschikbaar gesteld aan bevoegde gebruikers.

↓ Stap 5 Na maximaal één jaar worden persoonsgegevens automatisch geanonimiseerd.

↓ Stap 6 Alleen geanonimiseerde gegevens blijven beschikbaar.

7.11 Privacyrisico's Risico 1

Onbevoegde toegang Impact Middel Kans Laag Maatregelen

- autorisaties;
- TLS;
- beveiligde hosting;
- logging;
- toegangsbeheer.

Restrisico Laag.

Risico 2 Datalek Impact Middel Kans Laag Maatregelen

- datalekprotocol;
- monitoring;
- back-ups;
- incidentmanagement.

Restrisico Laag.

Risico 3 Verlies van gegevens Impact Middel Kans Laag Maatregelen

- back-ups;
- redundante opslag;
- herstelprocedures.

Restrisico Laag.

Risico 4 Onjuiste autorisaties Impact Middel Kans Laag Maatregelen

- rolgebaseerde autorisatie;
- periodieke controle;
- verwijdering van oude accounts.

Restrisico Laag.

Risico 5 Onnodig lange opslag Impact Middel Kans Zeer laag Maatregelen

- automatische anonimisering na één jaar.

Restrisico Zeer laag.

Risico 6 Herleidbaarheid van historische gegevens Na anonimisering zouden gegevens theoretisch opnieuw herleidbaar kunnen worden als de anonimisering onvoldoende effectief is.

Impact Hoog Kans Zeer laag Maatregelen

- alle direct identificerende gegevens (zoals naam en e-mailadres) worden verwijderd;
- indirect identificerende gegevens worden zodanig bewerkt of gegeneraliseerd dat redelijkerwijs geen herleiding tot een individu mogelijk is;
- de anonimisering is onomkeerbaar en er wordt geen koppeltabel of sleutel bewaard waarmee de gegevens opnieuw aan personen kunnen worden gekoppeld.

Restrisico Laag.

7.12 Technische maatregelen Onderwijsbekwaam B.V. past onder meer toe:

- TLS;
- beveiligde hosting;
- firewall;
- logging;
- monitoring;
- back-ups;
- software-updates;
- rolgebaseerde autorisaties;
- vulnerability management.

7.13 Organisatorische maatregelen Onderwijsbekwaam B.V. past onder meer toe:

- Privacy by Design;
- Privacy by Default;
- geheimhouding;
- autorisatiebeleid;
- dataminimalisatie;
- jaarlijkse evaluaties;
- periodieke risicoanalyse.

7.14 Beoordeling van de noodzaak van een formele DPIA

Op grond van de huidige inrichting is beoordeeld of de verwerking waarschijnlijk een hoog risico oplevert zoals bedoeld in artikel 35 AVG.

Bij deze beoordeling is onder meer gekeken naar:

- aard van de gegevens;
- omvang van de verwerking;
- betrokkenen;
- bewaartermijnen;
- profilering;
- geautomatiseerde besluitvorming;
- bijzondere persoonsgegevens;
- kwetsbare groepen.

Conclusie EQObserve:

- verwerkt slechts een beperkt aantal persoonsgegevens;
- verwerkt geen bijzondere persoonsgegevens;
- verwerkt geen gegevens van leerlingen;
- gebruikt geen profilering;
- gebruikt geen AI voor besluitvorming;
- verwijdert identificerende gegevens na maximaal één jaar door middel van onomkeerbare anonimisering.

Op basis hiervan is de verwerking naar verwachting niet aan te merken als een verwerking met een hoog restrisico die een voorafgaande raadpleging van de toezichthouder vereist. De onderwijsinstelling blijft als verwerkingsverantwoordelijke verantwoordelijk voor haar eigen beoordeling of, gelet op de wijze waarop zij EQObserve inzet, een aanvullende DPIA nodig is.

7.15 Restrisico

Na implementatie van de beschreven maatregelen wordt het restrisico beoordeeld als:

Laag Er zijn geen bekende restrisico's die onevenredig zijn ten opzichte van het doel van de verwerking.

7.16 Evaluatie Deze DPIA wordt opnieuw beoordeeld wanneer:

- nieuwe persoonsgegevens worden verwerkt;
- nieuwe functionaliteiten worden toegevoegd;
- AI-functionaliteit wordt geïntroduceerd;
- nieuwe subverwerkers worden ingezet;
- wetgeving wijzigt;
- zich een ernstig datalek of beveiligingsincident voordoet.

Daarnaast vindt minimaal eenmaal per jaar een evaluatie plaats.

7.17 Goedkeuring

Deze DPIA is vastgesteld door de directie van Onderwijsbekwaam B.V. en maakt integraal onderdeel uit van het Privacy-, Security- en Compliancehandboek.

Hoofdstuk 8

Incident Response & Datalekprotocol

8.1 Doel van dit protocol

Onderwijsbekwaam B.V., handelend onder de naam EQObserve, streeft naar een veilige, betrouwbare en continu beschikbare dienstverlening. Ondanks de getroffen technische en organisatorische beveiligingsmaatregelen kan zich een beveiligingsincident voordoen.

Dit Incident Response & Datalekprotocol beschrijft:

- hoe beveiligingsincidenten worden herkend;
- hoe incidenten worden geregistreerd;
- hoe de impact wordt beoordeeld;
- wanneer sprake is van een datalek;
- hoe incidenten worden afgehandeld;
- hoe wordt voldaan aan de verplichtingen uit de Algemene Verordening Gegevensbescherming (AVG).

Het protocol geldt voor alle medewerkers, ingehuurd professionals en leveranciers die betrokken zijn bij de dienstverlening van EQObserve.

8.2 Doelstellingen Het protocol heeft de volgende doelstellingen:

- het beperken van schade;
- het beschermen van persoonsgegevens;
- het waarborgen van de continuïteit van de dienstverlening;
- het voldoen aan de meldplicht datalekken;
- het voorkomen van herhaling van incidenten.

8.3 Definities Beveiligingsincident

Iedere gebeurtenis die de beschikbaarheid, integriteit of vertrouwelijkheid van informatie of systemen kan aantasten.

Voorbeelden:

- storing van de applicatie;
- malware;
- ransomware;
- ongeautoriseerde toegang;
- verlies van apparatuur;
- softwarefouten;
- menselijke fouten;
- netwerkindidenten.

Niet ieder beveiligingsincident is een datalek.

Datalek Een datalek is een inbreuk op de beveiliging die leidt tot:

- vernietiging;
- verlies;
- wijziging;
- ongeoorloofde verstrekking;
- ongeoorloofde toegang tot persoonsgegevens.

8.4 Rollen en verantwoordelijkheden Onderwijsbekwaam B.V.

Onderwijsbekwaam B.V. is verantwoordelijk voor:

- detectie van incidenten;
- registratie;
- eerste beoordeling;
- technische analyse;
- herstelmaatregelen;
- communicatie richting de onderwijsinstelling;
- documentatie.

Onderwijsinstelling De onderwijsinstelling is als verwerkingsverantwoordelijke verantwoordelijk voor:

- beoordeling van de meldplicht richting de Autoriteit Persoonsgegevens;
- eventuele melding aan betrokkenen;
- communicatie richting medewerkers.

Onderwijsbekwaam B.V. ondersteunt de onderwijsinstelling hierbij waar nodig.

8.5 Detectie van incidenten

Beveiligingsincidenten kunnen worden ontdekt door:

- monitoring;
- logging;
- gebruikersmeldingen;
- leveranciers;
- geautomatiseerde beveiligingssystemen;
- periodieke controles.

Iedere medewerker is verplicht een vermoedelijk beveiligingsincident onmiddellijk intern te melden.

8.6 Registratie

Van ieder beveiligingsincident wordt een incidentregistratie gemaakt.

Deze bevat minimaal:

- uniek incidentnummer;
- datum;

- tijdstip;
- melder;
- omschrijving;
- betrokken systemen;
- mogelijke persoonsgegevens;
- eerste beoordeling;
- genomen maatregelen;
- afsluitdatum.

De incidentregistratie wordt vertrouwelijk behandeld.

8.7 Classificatie van incidenten

Onderwijsbekwaam B.V. onderscheidt vier ernstniveaus.

Niveau Omschrijving Laag Beperkte impact, geen persoonsgegevens betrokken Middel Beperkte verstoring of beperkte blootstelling van persoonsgegevens Hoog Ernstige verstoring of waarschijnlijk datalek Kritiek Groot datalek, ernstige verstoring of continuïteitsrisico De classificatie bepaalt de prioriteit van de afhandeling.

8.8 Beoordeling Na melding wordt zo spoedig mogelijk beoordeeld:

- welke systemen zijn getroffen;
- welke persoonsgegevens mogelijk zijn geraakt;
- hoeveel betrokkenen mogelijk zijn getroffen;
- of gegevens zijn ingezien;
- of gegevens verloren zijn gegaan;
- of gegevens zijn gewijzigd;
- of gegevens openbaar zijn geworden;
- welke herstelmaatregelen noodzakelijk zijn.

8.9 Eerste maatregelen

Indien noodzakelijk worden direct maatregelen genomen.

Bijvoorbeeld:

- blokkeren van accounts;
- uitschakelen van systemen;
- herstellen van back-ups;
- wijzigen van wachtwoorden;
- afsluiten van netwerkverbindingen;
- blokkeren van ongeautoriseerde toegang.

Doel is verdere schade zoveel mogelijk te beperken.

8.10 Datalekbeoordeling

Na de eerste analyse wordt vastgesteld of sprake is van een datalek in de zin van artikel 4 AVG.

Hierbij wordt onder andere gekeken naar:

- aard van de persoonsgegevens;
- omvang;
- kans op misbruik;
- gevolgen voor betrokkenen;
- getroffen beveiligingsmaatregelen.

De beoordeling wordt schriftelijk vastgelegd.

8.11 Melding aan de onderwijsinstelling

Wanneer een beveiligingsincident betrekking heeft op persoonsgegevens die namens een onderwijsinstelling worden verwerkt, informeert Onderwijsbekwaam B.V. de betreffende onderwijsinstelling zonder onnodige vertraging nadat is vastgesteld dat sprake is van een (mogelijk) datalek.

Voor zover beschikbaar bevat deze melding ten minste:

- aard van het incident;
- datum en tijdstip van ontdekking;
- betrokken persoonsgegevens;
- vermoedelijke oorzaak;
- reeds genomen maatregelen;
- voorgestelde vervolgstappen;
- contactpersoon.

Indien nog niet alle informatie beschikbaar is, wordt de melding aangevuld zodra nieuwe informatie beschikbaar komt.

8.12 Melding aan de Autoriteit Persoonsgegevens

Omdat Onderwijsbekwaam B.V. in de meeste gevallen optreedt als verwerker, doet zij in beginsel geen zelfstandige melding aan de Autoriteit Persoonsgegevens.

De onderwijsinstelling beoordeelt als verwerkingsverantwoordelijke of een melding noodzakelijk is.

Onderwijsbekwaam B.V. verstrekt alle informatie die daarvoor nodig is.

Wanneer Onderwijsbekwaam B.V. voor een specifieke verwerking zelf verwerkingsverantwoordelijke is, beoordeelt zij zelfstandig of een melding aan de Autoriteit Persoonsgegevens vereist is.

8.13 Melding aan betrokkenen

Het informeren van betrokkenen is de verantwoordelijkheid van de onderwijsinstelling als verwerkingsverantwoordelijke.

Onderwijsbekwaam B.V. ondersteunt de onderwijsinstelling door:

- technische informatie beschikbaar te stellen;
- de omvang van het incident te analyseren;
- herstelmaatregelen toe te lichten;
- relevante documentatie aan te leveren.

8.14 Herstel

Na een incident worden passende herstelmaatregelen genomen.

Afhankelijk van het incident kunnen deze bestaan uit:

- herstellen van systemen;
- herstellen van gegevens;
- software-updates;
- extra beveiligingsmaatregelen;
- aanscherpen van autorisaties;
- aanvullende monitoring.

8.15 Evaluatie

Na afsluiting van ieder incident vindt een evaluatie plaats.

Hierbij wordt beoordeeld:

- oorzaak;
- effectiviteit van de reactie;
- verbetermaatregelen;
- noodzakelijke beleidsaanpassingen.

De uitkomsten worden vastgelegd.

8.16 Incidentregister

Onderwijsbekwaam B.V. houdt een intern incidentregister bij.

Per incident worden onder meer geregistreerd:

- datum;
- classificatie;
- oorzaak;
- impact;
- persoonsgegevens;
- maatregelen;
- evaluatie;
- afsluitdatum.

Dit register wordt gebruikt voor:

- interne evaluatie;
- verbetering van beveiliging;
- audits;
- aantoonbare naleving van de AVG.

8.17 Oefenen en testen

Onderwijsbekwaam B.V. beoordeelt periodiek of de incidentprocedures nog effectief zijn.

Waar passend worden:

- herstelprocedures getest;
- back-ups gecontroleerd;
- beveiligingsprocedures geëvalueerd.

Verbeterpunten worden verwerkt in dit protocol.

8.18 Samenwerking met leveranciers

Wanneer een incident ontstaat bij een subverwerker (zoals STRATO), werkt Onderwijsbekwaam B.V. samen met deze leverancier om:

- de oorzaak vast te stellen;
- de impact te beperken;
- de dienstverlening te herstellen;
- de onderwijsinstelling tijdig te informeren.

De afspraken hierover zijn vastgelegd in de overeenkomst met de betreffende subverwerker.

8.19 Continu verbeteren

Onderwijsbekwaam B.V. beschouwt ieder incident als een mogelijkheid om de dienstverlening verder te verbeteren.

Daarom worden:

- trends geanalyseerd;
- terugkerende oorzaken onderzocht;
- beveiligingsmaatregelen aangepast;
- procedures geactualiseerd.

8.20 Escalatiematrix Ernst Voorbeeld Actie

Laag Kleine storing zonder Registreren en oplossen tijdens persoonsgegevens reguliere werkzaamheden Middel Foutieve autorisatie of beperkte Direct onderzoek, herstelmaatregelen beschikbaarheidsproblemen en interne registratie Hoog Vermoedelijk datalek of Directe escalatie, informeren van de ongeautoriseerde toegang tot onderwijsinstelling en uitvoeren van persoonsgegevens impactanalyse Kritiek Bevestigd datalek met aanzienlijke Crisisrespons, voortdurende gevolgen of langdurige uitval van de communicatie met de dienstverlening onderwijsinstelling en ondersteuning bij wettelijke meldingen

8.21 Contact Beveiligingsincidenten kunnen worden gemeld via:

Onderwijsbekwaam B.V.

Handelend onder de naam EQObserve E-mail: info@eqobserve.com Meldingen worden met prioriteit behandeld.

8.22 Vaststelling en evaluatie

Dit Incident Response & Datalekprotocol is vastgesteld door de directie van Onderwijsbekwaam B.V. en maakt integraal onderdeel uit van het Privacy-, Security- en Compliancehandboek.

Het protocol wordt minimaal eenmaal per jaar geëvalueerd en daarnaast wanneer:

- de dienstverlening ingrijpend wijzigt;

- nieuwe beveiligingsrisico's worden vastgesteld;
- wet- en regelgeving verandert;
- een ernstig beveiligingsincident of datalek daartoe aanleiding geeft.

Hoofdstuk 9

Bewaar- en Vernietigingsbeleid

9.1 Doel van dit beleid

Onderwijsbekwaam B.V., handelend onder de naam EQObserve, verwerkt persoonsgegevens uitsluitend zolang dat noodzakelijk is voor de doeleinden waarvoor deze zijn verzameld.

Dit Bewaar- en Vernietigingsbeleid beschrijft:

- welke gegevens worden bewaard;
- hoe lang deze worden bewaard;
- wanneer gegevens worden verwijderd of geanonimiseerd;
- hoe anonimisering plaatsvindt;
- hoe wordt voorkomen dat persoonsgegevens langer worden bewaard dan noodzakelijk.

Dit beleid geeft uitvoering aan het beginsel van opslagbeperking zoals opgenomen in artikel 5, eerste lid, onder e, van de Algemene Verordening Gegevensbescherming (AVG).

9.2 Uitgangspunten

Onderwijsbekwaam B.V. hanteert de volgende uitgangspunten.

Dataminimalisatie Er worden uitsluitend persoonsgegevens verwerkt die noodzakelijk zijn voor de dienstverlening.

Opslagbeperking Persoonsgegevens worden niet langer bewaard dan noodzakelijk.

Privacy by Design De bewaartermijnen zijn onderdeel van het ontwerp van de applicatie.

Geautomatiseerde verwerking Waar mogelijk worden bewaartermijnen automatisch bewaakt.

Onomkeerbare anonimisering Na afloop van de bewaartermijn worden persoonsgegevens onomkeerbaar geanonimiseerd.

9.3 Persoonsgegevens binnen EQObserve

Binnen EQObserve worden uitsluitend de volgende persoonsgegevens verwerkt.

Persoonsgegeven Verwerking Naam Ja E-mailadres Ja Onderwijsinstelling Ja Afdeling Ja Leerjaar Ja Datum van Ja observatie Er worden geen bijzondere persoonsgegevens verwerkt.

9.4 Bewaartermijnen

Onderwijsbekwaam B.V. hanteert de volgende standaard bewaartermijnen.

Gegevenscategorie Bewaartermijn Actie na afloop Persoonsgegevens Maximaal 1 jaar **Onomkeerbare anonimisering Geanonimiseerde** Onbeperkt **Blijven beschikbaar observatiegegevens voor analyses Technische** Maximaal 12 maanden, tenzij langer **Verwijderen of loggegevens noodzakelijk voor onderzoek naar een** anonimiseren **beveiligingsincident** De bewaartermijn vangt aan op de datum waarop de observatie is geregistreerd.

9.5 Doel van de bewaartermijn

Onderwijsbekwaam B.V. hanteert voor persoonsgegevens binnen EQObserve een maximale bewaartermijn van één schooljaar, met een absolute maximumduur van één jaar.

Deze bewaartermijn is gebaseerd op het uitgangspunt van opslagbeperking zoals bedoeld in artikel 5, eerste lid, onder e, van de Algemene Verordening Gegevensbescherming (AVG).

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor het doel waarvoor zij zijn verzameld.

Binnen het onderwijs vinden observaties plaats in het kader van de professionele ontwikkeling van medewerkers gedurende een schooljaar. De resultaten worden gebruikt voor begeleiding, voortgangsgesprekken, evaluaties en kwaliteitsverbetering binnen diezelfde onderwijsperiode. Na afloop van het schooljaar neemt de noodzaak om de observaties nog tot individuele medewerkers te kunnen herleiden in beginsel af.

Daarom worden persoonsgegevens uiterlijk na één jaar automatisch en onomkeerbaar geanonimiseerd. Na deze anonimisering zijn de gegevens niet langer herleidbaar tot een natuurlijke persoon en kwalificeren zij niet langer als persoonsgegevens in de zin van de AVG.

De geanonimiseerde gegevens kunnen vervolgens worden bewaard en gebruikt voor:

- statistische analyses;
- trendanalyses over meerdere schooljaren;
- benchmarking op geaggregeerd niveau;
- kwaliteitsverbetering van de EQObserve-applicatie;
- wetenschappelijk en onderwijskundig onderzoek, voor zover uitsluitend gebruik wordt gemaakt van geanonimiseerde gegevens.

Met deze werkwijze wordt een evenwicht bereikt tussen enerzijds het ondersteunen van onderwijsinstellingen gedurende een volledig schooljaar en anderzijds het beperken van de bewaartermijn van persoonsgegevens overeenkomstig de beginselen van dataminimalisatie en opslagbeperking uit de AVG.

9.6 Anonimisering

Na afloop van de bewaartermijn worden persoonsgegevens automatisch en onomkeerbaar geanonimiseerd.

De anonimisering heeft tot doel de observatiegegevens beschikbaar te houden voor:

- kwaliteitsverbetering;
- trendanalyse;
- benchmarking;
- statistische analyses;
- onderwijskundig onderzoek.

Na anonimisering zijn de gegevens niet langer persoonsgegevens in de zin van de AVG.

9.7 Werkwijze bij anonimisering

Tijdens de anonimisering worden alle direct identificerende persoonsgegevens verwijderd uit de dataset.

Hieronder vallen onder meer:

- naam;
- e-mailadres.

Daarnaast worden indirect identificerende kenmerken zodanig verwerkt dat de gegevens redelijkerwijs niet meer tot een individuele medewerker zijn te herleiden.

Onderwijsbekwaam B.V. bewaart geen koppeltabel, sleutelbestand of andere technische voorziening waarmee geanonimiseerde gegevens opnieuw aan een individuele persoon kunnen worden gekoppeld.

Het anonimiseren is een definitieve en onomkeerbare handeling.

9.8 Verwijdering op verzoek

Gebruikers hebben het recht om, via de onderwijsinstelling of voor zover van toepassing rechtstreeks bij Onderwijsbekwaam B.V., een verzoek in te dienen tot verwijdering van hun persoonsgegevens.

Wanneer de onderwijsinstelling als verwerkingsverantwoordelijke opdracht geeft tot verwijdering, voert Onderwijsbekwaam B.V. deze zonder onnodige vertraging uit, tenzij een wettelijke verplichting of een zwaarwegend belang zich daartegen verzet.

Na verwijdering zijn de betreffende persoonsgegevens niet langer beschikbaar binnen de applicatie.

9.9 Back-ups

Persoonsgegevens kunnen gedurende een beperkte periode onderdeel uitmaken van beveiligde systeemback-ups.

Back-ups worden uitsluitend gebruikt voor:

- herstel na storingen;
- herstel na calamiteiten;
- waarborging van de continuïteit van de dienstverlening.

Back-ups worden niet gebruikt om verwijderde persoonsgegevens opnieuw beschikbaar te maken in de productieomgeving, tenzij dit noodzakelijk is voor het herstel van de gehele omgeving na een calamiteit. Indien een back-up wordt teruggezet, worden eventuele verwijderings- of anonimiseeracties zo spoedig mogelijk opnieuw uitgevoerd.

9.10 Geanonimiseerde gegevens

Na anonimisering blijven uitsluitend gegevens beschikbaar die niet langer tot individuele personen zijn te herleiden.

Deze gegevens worden gebruikt voor:

- statistiek;
- trendonderzoek;
- benchmarking;
- kwaliteitsverbetering van EQObserve;
- verbetering van observatiemethodieken.

Omdat deze gegevens geen persoonsgegevens meer bevatten, zijn de bepalingen van de AVG daarop niet langer van toepassing.

9.11 Vernietiging van gegevens

Wanneer persoonsgegevens niet worden geanonimiseerd, worden zij op een veilige wijze verwijderd.

Onderwijsbekwaam B.V. ziet erop toe dat persoonsgegevens niet onnodig blijven bestaan in:

- databases;

- exports;
- tijdelijke opslag;
- testomgevingen.

Persoonsgegevens worden niet gebruikt in testomgevingen, tenzij dit strikt noodzakelijk is en passende beveiligingsmaatregelen zijn getroffen. Waar mogelijk worden voor testdoeleinden uitsluitend geanonimiseerde of synthetische gegevens gebruikt.

9.12 Verantwoordelijkheden Onderwijsbekwaam B.V.

Onderwijsbekwaam B.V. is verantwoordelijk voor:

- uitvoering van de bewaartermijnen;
- automatische anonimisering;
- veilige verwijdering;
- beheer van het bewaarbeleid;
- periodieke controle op naleving.

Onderwijsinstelling De onderwijsinstelling is verantwoordelijk voor:

- de rechtmatigheid van de verwerking;
- het geven van instructies omtrent verwijdering indien noodzakelijk;
- het informeren van betrokkenen over de bewaartermijnen.

9.13 Controle Onderwijsbekwaam B.V. controleert periodiek of:

- persoonsgegevens niet langer worden bewaard dan toegestaan;
- anonimisering correct wordt uitgevoerd;
- verwijderde gegevens niet opnieuw beschikbaar zijn;
- het bewaarbeleid correct wordt toegepast.

Afwijkingen worden geregistreerd en zo spoedig mogelijk gecorrigeerd.

9.14 Wettelijke uitzonderingen

Indien een wettelijke verplichting een langere bewaartermijn voorschrijft, prevaleert die wettelijke verplichting boven de in dit beleid opgenomen standaardtermijnen.

Op het moment van vaststelling van dit handboek zijn voor de persoonsgegevens die binnen EQObserve worden verwerkt geen specifieke wettelijke bewaartermijnen bekend die afwijken van de in dit beleid opgenomen termijn van één jaar.

9.15 Evaluatie

Dit Bewaar- en Vernietigingsbeleid wordt minimaal eenmaal per jaar geëvalueerd.

Daarnaast wordt het beleid opnieuw beoordeeld wanneer:

- de dienstverlening wijzigt;
- nieuwe persoonsgegevens worden verwerkt;
- wet- en regelgeving verandert;
- nieuwe beveiligingsrisico's worden vastgesteld.

9.16 Samenvatting bewaarbeleid Gegevens Bewaartermij Eindactie

n Naam Maximaal 1 Anonimiseren jaar E-mailadres Maximaal 1 Anonimiseren jaar Onderwijsinstelling Maximaal 1 Anonimiseren jaar Afdeling Maximaal 1 Anonimiseren jaar Leerjaar Maximaal 1 Anonimiseren jaar Observatiedatum Maximaal 1 Anonimiseren als deze nog tot een individuele jaar medewerker herleidbaar is; daarna alleen geanonimiseerd bewaren Geanonimiseerde Onbeperkt Behouden voor statistische doeleinden observatiegegevens

9.17 Vaststelling

Dit Bewaar- en Vernietigingsbeleid is vastgesteld door de directie van Onderwijsbekwaam B.V. en maakt integraal onderdeel uit van het Privacy-, Security- en Compliancehandboek.

Hoofdstuk 10

Cookie Statement

10.1 Doel van dit Cookie Statement

Onderwijsbekwaam B.V., handelend onder de naam EQObserve, maakt binnen haar website en applicatie uitsluitend gebruik van cookies en vergelijkbare technieken die noodzakelijk zijn voor een veilige en correcte werking van de dienstverlening, tenzij uitdrukkelijk anders vermeld.

Dit Cookie Statement beschrijft:

- welke cookies worden gebruikt;
- waarom deze worden gebruikt;
- hoe lang deze worden bewaard;
- welke keuzes gebruikers hebben.

Dit Cookie Statement is opgesteld overeenkomstig:

- de Algemene Verordening Gegevensbescherming (AVG);
- de Telecommunicatiewet;
- de Europese ePrivacy-regelgeving.

10.2 Wat zijn cookies?

Cookies zijn kleine tekstbestanden die tijdens het bezoek aan een website of webapplicatie op een apparaat worden opgeslagen.

Cookies maken het mogelijk om een gebruiker tijdens een sessie te herkennen en bepaalde instellingen te onthouden.

Naast cookies kunnen vergelijkbare technieken worden gebruikt, zoals sessieopslag (session storage) of lokale opslag (local storage). Voor de leesbaarheid worden deze technieken in dit document gezamenlijk aangeduid als "cookies".

10.3 Uitgangspunt van EQObserve

EQObserve is ontwikkeld volgens het principe van Privacy by Default.

Daarom gebruikt EQObserve uitsluitend cookies die noodzakelijk zijn voor:

- veilige authenticatie;
- sessiebeheer;
- beveiliging van de applicatie;
- correcte werking van de software.

Er worden standaard geen trackingcookies, advertentiecookies of cookies voor gepersonaliseerde marketing geplaatst.

10.4 Welke cookies gebruikt EQObserve?

1. Functionele cookies Deze cookies zijn noodzakelijk voor het functioneren van de applicatie.

Voorbeelden:

- onthouden van een actieve sessie;
- beveiligde authenticatie;
- navigatie binnen de applicatie;
- bescherming tegen misbruik.

Zonder deze cookies functioneert EQObserve niet correct.

Toestemming vereist Nee.

2. Beveiligingscookies Deze cookies ondersteunen de beveiliging van de applicatie.

Voorbeelden:

- bescherming tegen sessiekaping;
- bescherming tegen Cross Site Request Forgery (CSRF);
- sessievalidatie;
- verificatie van ingelogde gebruikers.

Toestemming vereist Nee.

3. Voorkeurscookies Wanneer de applicatie gebruikersinstellingen onthoudt (zoals taalvoorkeur of weergave-instellingen), kunnen hiervoor voorkeurscookies worden gebruikt.

Deze cookies verbeteren uitsluitend het gebruiksgemak.

Toestemming vereist In beginsel nee, voor zover zij uitsluitend noodzakelijk zijn om een door de gebruiker gevraagde functionaliteit te leveren.

10.5 Cookies die EQObserve niet gebruikt

Onderwijsbekwaam B.V. gebruikt binnen de applicatie geen:

- advertentiecookies;
- marketingcookies;
- trackingcookies van advertentienetwerken;
- cookies voor behavioural advertising;
- social media trackingcookies;
- third-party trackingpixels;
- fingerprintingtechnieken voor marketingdoeleinden.

Persoonsgegevens worden niet gedeeld met advertentieplatformen.

10.6 Analytische cookies

Op dit moment maakt EQObserve geen gebruik van analytische cookies waarmee individuele gebruikers worden gevolgd.

Indien in de toekomst analytische cookies worden ingezet, zullen deze zo privacyvriendelijk mogelijk worden ingericht. Wanneer daarvoor op grond van de toepasselijke wetgeving toestemming is vereist, zal deze vooraf worden gevraagd.

10.7 Cookies van derden

Binnen de EQObserve-applicatie worden geen cookies geplaatst door derden voor commerciële of marketingdoeleinden.

Indien in de toekomst functionaliteit van derden wordt geïntegreerd waarbij cookies worden geplaatst, zal:

- dit Cookie Statement worden aangepast;
- indien wettelijk vereist vooraf toestemming worden gevraagd.

10.8 Bewaartermijnen

EQObserve hanteert zo kort mogelijke bewaartermijnen.

Type cookie Maximale bewaartermijn Sessiecookies Tot het einde van de browsersessie Beveiligingscookies Maximaal de duur van de sessie of zolang noodzakelijk voor de beveiligingsfunctie Voorkeurscookies Maximaal 12 maanden, tenzij de gebruiker de instellingen eerder wijzigt of verwijdt Cookies worden niet langer bewaard dan noodzakelijk is voor het doel waarvoor zij zijn geplaatst.

10.9 Browserinstellingen

Gebruikers kunnen cookies beheren via de instellingen van hun browser.

Het uitschakelen van functionele cookies kan ertoe leiden dat:

- inloggen niet meer mogelijk is;
- sessies voortijdig worden beëindigd;
- delen van de applicatie niet correct functioneren.

Onderwijsbekwaam B.V. kan in dat geval de goede werking van de applicatie niet garanderen.

10.10 Lokale opslag

De applicatie kan gebruikmaken van browsertechnieken zoals Local Storage of Session Storage voor tijdelijke opslag van technische gegevens die noodzakelijk zijn voor het functioneren van de applicatie.

Deze gegevens worden niet gebruikt voor marketing of profilering.

Waar deze technieken persoonsgegevens bevatten, worden zij met dezelfde zorg behandeld als cookies.

10.11 Beveiliging

Cookies worden uitsluitend gebruikt binnen beveiligde verbindingen (HTTPS/TLS).

Onderwijsbekwaam B.V. neemt passende maatregelen om misbruik van cookies te voorkomen.

Waar technisch mogelijk worden beveiligingskenmerken toegepast, zoals:

- Secure (uitsluitend verzending via HTTPS);
- HttpOnly (niet toegankelijk via client-side scripts voor sessiecookies);
- SameSite (bescherming tegen Cross-Site Request Forgery).

De gekozen instellingen worden afgestemd op de functionaliteit en de beveiligingsbehoefte van de applicatie.

10.12 Toestemming

Voor cookies die strikt noodzakelijk zijn voor het functioneren en beveiligen van de applicatie is op grond van de geldende wetgeving geen toestemming vereist.

Mocht Onderwijsbekwaam B.V. in de toekomst niet-noodzakelijke cookies gaan gebruiken, dan zullen deze pas worden geplaatst nadat de gebruiker – voor zover wettelijk vereist – hiervoor toestemming heeft gegeven.

Gebruikers kunnen een eerder gegeven toestemming op ieder moment intrekken.

10.13 Wijzigingen

Onderwijsbekwaam B.V. kan dit Cookie Statement aanpassen wanneer:

- nieuwe functionaliteiten worden toegevoegd;
- nieuwe cookies worden gebruikt;
- wet- en regelgeving verandert;
- technische ontwikkelingen daartoe aanleiding geven.

De meest actuele versie is steeds beschikbaar via de website van EQObserve.

10.14 Contact

Voor vragen over dit Cookie Statement of het gebruik van cookies kunt u contact opnemen met:

Onderwijsbekwaam B.V.

Handelend onder de naam EQObserve E-mail: info@eqobserve.com

10.15 Samenvatting

EQObserve gebruikt uitsluitend cookies en vergelijkbare technieken die noodzakelijk zijn voor:

- veilige authenticatie;
- sessiebeheer;
- beveiliging van de applicatie;
- het correct functioneren van de software.

EQObserve gebruikt geen:

- advertentiecookies;
- marketingcookies;
- trackingcookies;
- profilering;
- social media tracking.

Hierdoor is het gebruik van de applicatie zo privacyvriendelijk mogelijk ingericht.

10.16 Vaststelling

Dit Cookie Statement is vastgesteld door de directie van Onderwijsbekwaam B.V. en maakt integraal onderdeel uit van het Privacy-, Security- en Compliancehandboek.

Hoofdstuk 11

AI- en Algoritmeverklaring

11.1 Doel van deze verklaring

Onderwijsbekwaam B.V., handelend onder de naam EQObserve, vindt het belangrijk transparant te zijn over de wijze waarop de applicatie gebruikmaakt van algoritmen, geautomatiseerde processen en – indien van toepassing – kunstmatige intelligentie (Artificial Intelligence, AI).

Deze verklaring beschrijft:

- welke geautomatiseerde technieken binnen EQObserve worden toegepast;
- waarvoor deze technieken worden gebruikt;
- waarvoor zij nadrukkelijk niet worden gebruikt;
- hoe de rechten van gebruikers worden beschermd.

Deze verklaring sluit aan bij de uitgangspunten van de Algemene Verordening Gegevensbescherming (AVG), de EU AI Act en de beginselen van verantwoord gebruik van AI.

11.2 Uitgangspunten

Onderwijsbekwaam B.V. hanteert de volgende uitgangspunten bij de ontwikkeling van EQObserve:

- menselijke beoordeling staat centraal;
- transparantie;
- uitlegbaarheid;
- proportionaliteit;
- privacy by design;
- dataminimalisatie;
- veiligheid;
- betrouwbaarheid.

EQObserve ondersteunt onderwijsprofessionals, maar neemt geen beslissingen namens hen.

11.3 Gebruik van algoritmen

Binnen EQObserve worden geautomatiseerde processen gebruikt voor de normale werking van de applicatie.

Voorbeelden hiervan zijn:

- authenticatie;
- autorisatie;
- genereren van rapportages;
- verwerken van observatiegegevens;
- statistische berekeningen;

- geanonimiseerde trendanalyses.

Deze processen zijn bedoeld om gegevens efficiënt te verwerken en rapportages beschikbaar te maken.

11.4 Geen geautomatiseerde besluitvorming

EQObserve neemt geen geautomatiseerde besluiten die rechtsgevolgen hebben of gebruikers anderszins in aanmerkelijke mate treffen, zoals bedoeld in artikel 22 AVG.

Er worden geen besluiten genomen over:

- functioneren van medewerkers;
- beoordelingen;
- arbeidsrechtelijke gevolgen;
- promoties;
- salaris;
- disciplinaire maatregelen;
- inzetbaarheid.

Alle beslissingen blijven de verantwoordelijkheid van de onderwijsinstelling en de daarvoor bevoegde personen.

11.5 Geen profilering

EQObserve past geen profilering toe zoals bedoeld in de AVG.

Persoonsgegevens worden niet gebruikt om:

- persoonlijk gedrag te voorspellen;
- persoonlijkheidsprofielen op te stellen;
- risico-inschattingen van medewerkers te maken;
- individuele prestaties automatisch te beoordelen.

De applicatie genereert uitsluitend rapportages op basis van ingevoerde observatiegegevens.

11.6 Gebruik van AI

Op het moment van vaststelling van dit handboek maakt EQObserve geen gebruik van generatieve kunstmatige intelligentie (Generative AI) of andere AI-systemen voor het verwerken van persoonsgegevens van gebruikers.

Er worden geen persoonsgegevens gebruikt voor:

- het trainen van AI-modellen;
- het verbeteren van taalmodellen;
- commerciële AI-doeleinden;
- externe AI-diensten.

Persoonsgegevens worden uitsluitend verwerkt voor de in dit handboek beschreven doeleinden.

11.7 Toekomstig gebruik van AI

Indien Onderwijsbekwaam B.V. in de toekomst AI-functionaliteit toevoegt aan EQObserve, zal vooraf worden beoordeeld:

- welk doel de AI-functionaliteit dient;

- welke persoonsgegevens worden verwerkt;
- welke risico's dit oplevert voor betrokkenen;
- of een aanvullende DPIA noodzakelijk is;
- of aanvullende informatie aan gebruikers moet worden verstrekt.

Nieuwe AI-functionaliteit zal pas in gebruik worden genomen nadat is vastgesteld dat deze voldoet aan de toepasselijke wet- en regelgeving.

11.8 Transparantie

Gebruikers hebben recht op duidelijke informatie over de werking van de applicatie.

Wanneer geautomatiseerde analyses worden toegepast, wordt inzichtelijk gemaakt:

- welke gegevens worden gebruikt;
- met welk doel de analyse plaatsvindt;
- hoe de uitkomsten tot stand komen, voor zover dit redelijkerwijs mogelijk is.

Onderwijsbekwaam B.V. streeft ernaar dat geautomatiseerde processen begrijpelijk en controleerbaar zijn.

11.9 Menselijke tussenkomst

Alle interpretatie van observaties en alle beslissingen die gevolgen kunnen hebben voor medewerkers worden genomen door bevoegde personen binnen de onderwijsinstelling.

EQObserve ondersteunt deze besluitvorming uitsluitend door informatie overzichtelijk beschikbaar te maken.

Gebruikers kunnen geautomatiseerd gegenereerde rapportages beoordelen, bespreken en – waar nodig – aanvullen met eigen professionele inzichten.

11.10 Kwaliteit van gegevens

De kwaliteit van rapportages is afhankelijk van de juistheid van de ingevoerde gegevens.

Onderwijsbekwaam B.V. is niet verantwoordelijk voor:

- onjuiste invoer;
- onvolledige observaties;
- onjuiste interpretaties van rapportages;
- beslissingen die door gebruikers of onderwijsinstellingen worden genomen op basis van de beschikbare informatie.

Gebruikers blijven verantwoordelijk voor de inhoud van de ingevoerde observaties.

11.11 Voorkomen van bias

Onderwijsbekwaam B.V. streeft ernaar dat de applicatie geen ongewenste vooroordelen (bias) introduceert.

Omdat EQObserve geen AI gebruikt voor het beoordelen of classificeren van personen, is het risico op algoritmische discriminatie beperkt.

Wanneer in de toekomst AI-functionaliteit wordt toegevoegd, zal bijzondere aandacht worden besteed aan:

- representativiteit van gegevens;
- uitlegbaarheid;
- controleerbaarheid;

- menselijke toetsing;
- periodieke evaluatie van uitkomsten.

11.12 Beveiliging van gegevens

Alle persoonsgegevens die binnen EQObserve worden verwerkt, worden beschermd overeenkomstig het Informatiebeveiligingsbeleid zoals beschreven in hoofdstuk 4 van dit handboek.

AI-functionaliteit zal nooit leiden tot een lager beveiligingsniveau dan voor overige onderdelen van de applicatie geldt.

11.13 Gebruik van geanonimiseerde gegevens

Na afloop van de bewaartermijn worden persoonsgegevens volledig en onomkeerbaar geanonimiseerd.

Geanonimiseerde gegevens kunnen worden gebruikt voor:

- statistische analyses;
- kwaliteitsverbetering;
- benchmarking;
- trendonderzoek.

Deze gegevens zijn niet langer herleidbaar tot individuele personen.

Indien Onderwijsbekwaam B.V. in de toekomst geanonimiseerde gegevens wil gebruiken voor de ontwikkeling of verbetering van algoritmen of AI-functionaliteit, zal dit uitsluitend plaatsvinden met datasets die redelijkerwijs niet meer tot natuurlijke personen zijn te herleiden.

11.14 Naleving van wet- en regelgeving

Onderwijsbekwaam B.V. volgt de ontwikkelingen rondom Europese regelgeving op het gebied van kunstmatige intelligentie en gegevensbescherming.

Voor zover van toepassing wordt de dienstverlening ingericht overeenkomstig:

- de Algemene Verordening Gegevensbescherming (AVG);
- de Uitvoeringswet AVG (UAVG);
- de EU AI Act;
- overige toepasselijke Europese en Nederlandse wet- en regelgeving.

Nieuwe functionaliteiten worden vooraf getoetst aan deze regelgeving.

11.15 Verantwoordelijkheden Onderwijsbekwaam B.V.

Onderwijsbekwaam B.V. is verantwoordelijk voor:

- een veilige en betrouwbare technische inrichting van EQObserve;
- transparantie over het gebruik van algoritmen en AI;
- naleving van toepasselijke wet- en regelgeving;
- periodieke evaluatie van geautomatiseerde processen.

Onderwijsinstelling De onderwijsinstelling is verantwoordelijk voor:

- de wijze waarop rapportages worden gebruikt;
- de interpretatie van observaties;

- personeelsbesluiten;
- communicatie met medewerkers over het gebruik van EQObserve.

11.16 Evaluatie

Deze AI- en Algoritmeverklaring wordt minimaal eenmaal per jaar geëvalueerd.

Daarnaast vindt een tussentijdse evaluatie plaats wanneer:

- AI-functionaliteit wordt toegevoegd;
- wet- en regelgeving wijzigt;
- nieuwe risico's worden vastgesteld;
- de dienstverlening wezenlijk verandert.

11.17 Contact

Voor vragen over deze AI- en Algoritmeverklaring of over de wijze waarop EQObserve gebruikmaakt van geautomatiseerde processen kunt u contact opnemen met:

Onderwijsbekwaam B.V.

Handelend onder de naam EQObserve E-mail: info@eqobserve.com

11.18 Vaststelling

Deze AI- en Algoritmeverklaring is vastgesteld door de directie van Onderwijsbekwaam B.V.

en maakt integraal onderdeel uit van het Privacy-, Security- en Compliancehandboek.