

## Programma van Eisen GRC-oplossing funderend onderwijs

---

Versie: 1.0

TLP: **GREEN:** openbaar inzichtelijk, maar alleen te gebruiken  
binnen het kader van deelname aan een aanbesteding.

---

## Definities:

In dit Programma van Eisen wordt, tenzij uit de context uitdrukkelijk anders blijkt, verstaan onder:

**AVG:** de Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679).

**EER:** de Europese Economische Ruimte, bestaande uit de lidstaten van de Europese Unie plus IJsland, Liechtenstein en Noorwegen.

**FO/Funderend Onderwijs:** het primair onderwijs en voortgezet onderwijs in Nederland.

**Gebruiker:** de gebruikers van de Oplossing bij Opdrachtgever.

**Hoofdovereenkomst:** de (raam)overeenkomst die tussen Opdrachtnemer en Opdrachtgever van toepassing is op de levering van de Oplossing, daaronder begrepen eventuele Service Level Agreement(s), licentievoorwaarden en/of algemene voorwaarden van Opdrachtnemer, alsmede iedere verlenging, vernieuwing of vervanging daarvan.

**Model Verwerkersovereenkomst:** de op enig moment meest recente versie van de modelverwerkersovereenkomst behorend bij het Convenant Digitale Onderwijsmiddelen en Privacy, zoals gepubliceerd op [www.privacyconvenant.nl](http://www.privacyconvenant.nl).

**Normenkader IBP-FO:** het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs, in de op enig moment geldende actuele versie.

**Opdrachtgever:** het afnemend schoolbestuur binnen het Funderend Onderwijs dat de Oplossing afneemt van Opdrachtnemer.

**Opdrachtnemer:** de leverancier van de Oplossing.

**Oplossing/GRC-oplossing:** de door Opdrachtnemer aangeboden en door Opdrachtgever afgenomen Governance, Risk & Compliance-oplossing waarop dit Programma van Eisen betrekking heeft.

**Overeenkomst:** de Hoofdovereenkomst en/of de overeenkomst waarmee de toepasselijkheid van dit PvE tussen Opdrachtgever en Opdrachtnemer wordt vastgelegd, waarbij dit Programma van Eisen in alle gevallen integraal onderdeel daarvan uitmaakt.

**Programma van Eisen/PvE:** dit document, inclusief eventuele bijlagen.

**Verwerkersovereenkomst:** de overeenkomst als bedoeld in artikel 28 AVG die Opdrachtnemer als verwerker met Opdrachtgever als verwerkingsverantwoordelijke sluit, op basis van de Model Verwerkersovereenkomst.

## 1 Eisen – Algemeen

### 1.1 Algemeen

In dit Programma van Eisen zijn de minimale kwaliteitsstandaarden beschreven waar de af te nemen GRC-oplossing aan dient te voldoen. Binnen de Oplossing ligt de verantwoordelijkheid voor een correcte werking en ondersteuning van de Oplossing gedurende de volledige contractperiode bij de leverancier van de GRC-oplossing (in dit document aangeduid als Opdrachtnemer). Correcte werking ziet op de technische en functionele werking van de Oplossing volgens de in dit Programma van Eisen gestelde eisen en zoals door Opdrachtnemer aangeboden. Dit laat onverlet dat de juistheid van door Opdrachtgever of Gebruikers ingevoerde gegevens, gemaakte configuratiekeuzes, juist gebruik door Opdrachtgever of Gebruikers van de Oplossing volgens de voorschriften van Opdrachtnemer en overige aan Opdrachtgever en haar Gebruikers toebedeelde verantwoordelijkheden de verantwoordelijkheid van Opdrachtgever betreft.

### 1.2 Partnerschap en samenwerking

Opdrachtnemer draagt actief bij aan een goed partnerschap met Opdrachtgever. Hieronder kan bijvoorbeeld worden verstaan:

- Proactieve communicatie en transparantie over o.a. ontwikkelingen, risico's en kansen, marktontwikkelingen, etc.;
- Samenwerking en afstemming via tactische en operationele overleggen om de dienstverlening blijvend te onderhouden en ontwikkelen;
- Flexibiliteit en betrouwbaarheid: meebewegen bij veranderende behoeften van scholen of van Opdrachtgever.

### 1.3 Naleving wet- en regelgeving

De oplossing en ondersteuning voldoet steeds ten tijde van aanbieden c.q. ingebruikname en gedurende de volledige looptijd van de Overeenkomst aan de geldende wet- en regelgeving in Nederland. Als tijdens de looptijd gewijzigde wet- en regelgeving aanpassingen noodzakelijk maakt, zal Opdrachtnemer deze tijdig (indien van toepassing binnen de door wet- en regelgeving gestelde tijdslijnen) en zonder meerkosten doorvoeren, voor zover dit redelijkerwijs binnen de invloedssfeer van Opdrachtnemer ligt.

### 1.4 Informatiebeveiliging

Opdrachtnemer dient te beschikken over een hoogwaardig systeem voor informatie en databeveiliging en dient voldoende maatregelen te hebben getroffen op het gebied van informatiebeveiliging. Hiertoe dient Opdrachtnemer te beschikken over een geldig ISO 27001-certificaat of gelijkwaardige toepasselijke waarborging/certificaat waaruit blijkt dat haar organisatie en dienstverlening voldoen aan de daarin gestelde beveiligingseisen. De waarborging/ certificering dient minimaal te zijn op de relevante dienstverlening voor de Oplossing, waaronder ontwikkeling, beheer, hosting en support.

Op verzoek van Opdrachtgever wordt hiervoor een geldig kwaliteitscertificaat van een geaccrediteerde certificeringsinstelling overlegd dat gebaseerd is op de ISO 27001 of gelijkwaardige standaard voor informatiebeveiliging, waaruit blijkt dat de organisatie en storage(locaties) van Opdrachtnemer voldoen aan de daarin gestelde hoogwaardige beveiligingseisen.

Het certificaat dient geldig te zijn gedurende de looptijd van de Overeenkomst. Opdrachtnemer informeert Opdrachtgever bij verlenging, verval, schorsing of intrekking van het certificaat tijdig en proactief.

Ingeval van overlegging van een 'gelijkwaardige' certificering, dient dit gepaard te gaan met de daarbij behorende verklaring van toepasselijkheid of gelijkwaardig. De bewijslast voor deze gelijkwaardigheid berust bij Opdrachtnemer.

## **1.5 AVG**

Opdrachtnemer dient aantoonbaar te voldoen aan de vereisten van de Algemene Verordening Gegevensbescherming (AVG). Persoonsgegevens die binnen de aangeboden oplossing worden opgeslagen, verwerkt of gemonitord, dan wel door eventueel door Opdrachtnemer ingezette sub verwerkers, dienen uitsluitend te worden verwerkt binnen datacenters die zijn gevestigd in de Europese Economische Ruimte (EER). Toegang tot persoonsgegevens vanuit landen buiten de EER is uitsluitend toegestaan als daarbij een passend beschermingsniveau volgens de AVG is gewaarborgd.

Opdrachtnemer informeert Opdrachtgever onverwijld en uiterlijk binnen 24 uur na ontdekking van een incident of datalek waarbij de dienstverlening en/of persoonsgegevens van Opdrachtgever zijn betrokken, inclusief de aard van het incident, de betrokken categorieën persoonsgegevens, de (mogelijke) gevolgen en de getroffen maatregelen.

## **1.6 Aansprakelijkheidsverzekering**

Opdrachtnemer is gedurende de looptijd van de opdracht afdoende verzekerd tegen bedrijfsaansprakelijkheid- en cyber-/datarisico's. Op verzoek van Opdrachtgever verstrekt Opdrachtnemer een geldig polisblad of een assurantieverklaring waaruit de dekking blijkt.

Opdrachtnemer beschikt hierbij over verzekeringen met minimaal de volgende dekking:

- Bedrijfsaansprakelijkheidsverzekering met een minimale dekking van € 1.000.000, - per aanspraak;
- Cyber-/datarisicoverzekering met een minimale dekking van € 500.000, - per aanspraak.

## **1.7 Ondersteuning en actualisatie Normenkader IBP-FO**

De Oplossing dient de meeste actuele versie van het Normenkader Informatiebeveiliging en Privacy Funderend Onderwijs (IBP-FO) volledig te ondersteunen. Onder ondersteunen wordt in deze verstaan dat de Oplossing de Gebruiker in staat stelt om via de tooling volledige en volwaardige invulling te geven

aan de zelf-evaluatie en monitoring van de implementatie van het Normenkader IBP-FO, waarbij de tooling uitgaat van de meest actuele versie.

De Oplossing dient Opdrachtgever en haar Gebruikers in staat te stellen om vast te stellen of wijzigingen in het Normenkader, onderliggende wet- en regelgeving en/of relevante richtlijnen zijn doorgevoerd. Hierbij geldt dat:

- Het voor de Gebruiker mogelijk dient te zijn om te toetsen en/of in te zien binnen de Oplossing of het Normenkader IBP-FO is geüpdatet;
- Formele, gepubliceerde wijzigingen ten aanzien van het Normenkader IBP-FO binnen vier (4) weken na de officiële publicatie en/of inwerkingtreding aantoonbaar verwerkt zijn in de oplossing;
- De Oplossing deze wijzigingen en de doorgevoerde actualisaties inzichtelijk maakt voor Gebruikers en, indien dit noodzakelijk blijkt vanuit een doorgevoerde wijziging/actualisatie, melding maakt naar Gebruikers om een norm opnieuw te toetsen op volwassenheidsniveau.

## **1.8 Verwerkersovereenkomst**

Bij aanvang van de Overeenkomst tekent Opdrachtnemer de door Opdrachtgever gehanteerde Model-Verwerkersovereenkomst. Hierbij wordt in uitgegaan van de meest recente versie van de [Model Verwerkersovereenkomst](#) behorend bij het Convenant Digitale Onderwijsmiddelen en Privacy, tenzij hierover expliciet andere afspraken worden gemaakt tussen Opdrachtgever en Opdrachtnemer. Het gebruik van een andere verwerkersovereenkomst dient te allen tijde expliciet geaccordeerd te worden door Opdrachtgever.

## **1.9 Intellectueel eigendom ingevoerde data**

Alle door Opdrachtgever ingevoerde, gegenereerde of beheerde gegevens, documenten en overige content blijven te allen tijde eigendom van Opdrachtgever. Het gebruik van deze gegevens door Opdrachtnemer is uitsluitend toegestaan voor zover noodzakelijk voor de uitvoering van de dienstverlening.

## **1.10 Voertaal**

De GRC-oplossing, inclusief de beschikbare functionaliteiten, zijn beschikbaar in de Nederlandse taal, waarbij handleidingen, gebruikersinterfaces, standaardteksten, rapportages, dashboards, menu's en systeemmeldingen in het Nederlands worden aangeboden. Daarnaast dient de support- en servicedesk van Opdrachtnemer Nederlandstalig te communiceren met Gebruikers, zowel mondeling als schriftelijk.

## **1.11 Doorlegging informatiebeveiligingseisen**

Opdrachtnemer waarborgt dat de in dit Programma van Eisen gestelde informatiebeveiligingseisen eveneens worden nageleefd door eventuele door Opdrachtnemer ingeschakelde derden die betrokken zijn bij de levering van de Oplossing, en legt deze verplichtingen contractueel aan hen op.

## 2 Eisen – Functioneel en technisch

### 2.1 Software as a Service (SaaS)

De aangeboden GRC-oplossing wordt als Software-as-a-Service (SaaS) geleverd en is via het internet toegankelijk voor geautoriseerde Gebruikers van Opdrachtgever. De Oplossing ondersteunt ten minste de meest recente versies of één voorgaande hoofdversie van gangbare webbrowsers (minimaal Edge, Chrome, Firefox en Safari) en kan volledig worden gebruikt zonder digitale dan wel fysieke installatie van aanvullende software, browserextensies, plug-ins of andere lokale componenten op de werkplek van de Gebruiker.

### 2.2 Algemene randvoorwaarden – licenties, updates en upgrades

Opdrachtnemer draagt te allen tijde verantwoordelijkheid en zonder aanvullende kosten voor de beschikbaarheid en beschikbaarstelling van benodigde licenties, updates en upgrades. Updates en upgrades die volgen uit noodzakelijke security-, wettelijke- en/of Normenkaderupdates worden zonder aanvullende kosten dan wel licentie doorgevoerd in de Oplossing.

Functionaliteiten die onderdeel uitmaken van de Oplossing en licentie zoals afgenomen door Opdrachtgever bij aanvang van deze Overeenkomst worden door Opdrachtnemer niet eenzijdig, zonder akkoord van Opdrachtgever verwijderd uit de Oplossing, dan wel onbeschikbaar gemaakt voor Opdrachtgever en haar Gebruikers.

### 2.3 Algemene randvoorwaarden – AI-modellen

Indien in de dienstverlening AI-functionaliteit wordt toegepast, maakt Opdrachtnemer voorafgaand aan ingebruikname inzichtelijk welke AI-functionaliteiten onderdeel zijn van de Oplossing, met per AI-functionaliteit ten minste het beoogde doel, het gebruikte AI-systeem/AI-model en de toepasselijke kwalificatie en risicoclassificatie op grond van de AI-Verordening. Opdrachtnemer borgt dat deze AI-functionaliteit aantoonbaar veilig, betrouwbaar en controleerbaar functioneert.

Opdrachtnemer:

- Test periodiek (minimaal bij ingebruikname of bij ingrijpende wijzigingen ) de gebruikte AI-modellen op bias (mogelijk discriminerende of anderszins ongewenste uitkomsten), nauwkeurigheid, betrouwbaarheid en prestatie, en legt de resultaten vast in een toetsingsrapport;
- Documenteert de toegepaste testmethodiek en eventuele verbetermaatregelen, en stelt deze op verzoek beschikbaar aan Opdrachtgever;
- Test en valideert elke materiële wijziging of update van AI-modellen voorafgaand aan ingebruikname en informeert Opdrachtgever hier vooraf over, waaronder bij wijziging van het gebruikte model of de modelaanbieder;

- Levert bewijs van naleving op verzoek van Opdrachtgever, waaronder de informatie die Opdrachtgever redelijkerwijs nodig heeft om een DPIA en, indien van toepassing, een grondrechtenbeoordeling (FRIA) uit te voeren;
- Verleent op verzoek van Opdrachtgever medewerking aan een audit, DPIA, grondrechtenbeoordeling of onafhankelijke toetsing van de toegepaste AI-functionaliteit;
- Borgt dat gegevens die door Gebruikers worden ingevoerd, geüpload of verwerkt binnen de AI-functionaliteit, danwel output vloeiend uit handelingen van Gebruikers niet worden gebruikt voor het trainen, verbeteren of ontwikkelen van AI-modellen van Opdrachtnemer of derden;
- Waarborgt menselijk toezicht (art. 14 AI-Verordening) op de AI-functionaliteit, waarbij Gebruikers de AI-output kunnen beoordelen, negeren, corrigeren of het gebruik kunnen beëindigen, en besluitvorming niet uitsluitend op basis van AI-output plaatsvindt zonder menselijke beoordeling en goedkeuring;
- Voldoet aan de toepasselijke transparantieplichtingen van artikel 50 AI-Verordening, waaronder waar van toepassing het informeren van betrokkenen dat zij met een AI-systeem interageren en het markeren van AI-gegenereerde content.

Indien een AI-functionaliteit kwalificeert als AI-systeem met een hoog risico, ook als deze bepalingen nog niet in werking zijn getreden, voldoet Opdrachtnemer tevens aan de overige op Opdrachtnemer toepasselijke verplichtingen uit de AI-Verordening en verstrekt hij Opdrachtgever de informatie die nodig is om aan haar verplichtingen als gebruiksverantwoordelijke te voldoen.

## 2.4 Toegangsbeheer en Authenticatie

De GRC-oplossing ondersteunt standaard authenticatie via Single Sign-On (SSO) met een centraal beheerde identity provider (bijvoorbeeld Microsoft 365, Google Workspace of gelijkwaardig) en autorisatie op basis van centraal beheerde gebruikersrollen. Als SSO niet mogelijk is, is multi-factor authenticatie (MFA) verplicht voor alle beheeraccounts en accounts met verhoogde rechten.

## 2.5 Autorisatie

De GRC-oplossing biedt een role-based autorisatiemodel (RBAC) waarmee gebruikers toegang krijgen tot gegevens en functionaliteiten op basis van door Opdrachtgever toegewezen rollen. Het autorisatiemodel maakt het mogelijk voor Opdrachtgever om toegangsrechten per aangesloten instelling of organisatie van Opdrachtgever onafhankelijk van elkaar in te richten, te beheren en af te schermen. Indien door Opdrachtgever als zijnde ingesteld, dienen Gebruikers enkel gegevens te zien waartoe zij gemachtigd/geautoriseerd zijn.

## 2.6 Wijziging- en releasebeleid

Opdrachtnemer hanteert een gestructureerd, gedocumenteerd proces voor ontwikkeling en wijzigingsbeheer. Nieuwe of gewijzigde functionaliteit wordt voor brede uitrol naar gebruikers getest binnen een afgebakende groep en op impact

beoordeeld. Significante, impactvolle wijzigingen worden vooraf aangekondigd, waarbij een minimale aankondigingstermijn geldt van tien (10) werkdagen. Uitzondering hierop zijn noodwijzigingen. Hierbij geldt hetgeen beschreven onder eis 4.4.

Gebruikers verkrijgen inzicht in de ontwikkelingen via een release-, wijziging-en/of ontwikkelingskalender.

Als een release ondanks de uitvoering van preventieve testen niet stabiel wordt bevonden of de gebruikservaring van de eindgebruiker significant negatief wordt beïnvloed, wordt voor zover mogelijk een rollback uitgevoerd naar de laatst werkende versie.

## **2.7 Kwalitatieve toelichting**

De Oplossing faciliteert om per norm, beheersmaatregel of beoordelingsonderdeel een kwalitatieve toelichting vast te leggen, te beheren en te wijzigen. De toelichting dient handmatig ingevoerd te worden en dient gewijzigd te kunnen worden door geautoriseerde Gebruikers. Herbeoordeling van normen dient hierbij mogelijk te zijn. De Oplossing dient versiebeheer op de toelichtingen te ondersteunen, waarbij minimaal wordt vastgelegd welke Gebruiker een toelichting heeft gegenereerd, gewijzigd, geüpload of ingediend, zodat minimaal voor geautoriseerde Gebruikers herleidbaar en inzichtelijk is wie op welk moment voorgenoemde handelingen heeft uitgevoerd.

## **2.8 Bewijsstukken**

De Oplossing dient de mogelijkheid te bieden om per norm, beheersmaatregel of beoordeling optioneel bewijsstukken, bijlagen en/of verwijzingen naar relevante documentatie te koppelen. De Oplossing dient gangbare bestandsformaten te ondersteunen (waaronder minimaal .pdf, .docx, .xlsx) en verwijzingen naar externe documentmanagementsystemen of URL's mogelijk te maken. Toegang tot gekoppelde bewijsstukken dient te zijn gebaseerd op autorisaties en rollen.

## **2.9 Validatie mogelijkheden**

De Oplossing dient functionaliteit te bieden voor een, al dan niet door Opdrachtgever instelbaar, proces ter waarborging van de volledigheid en tijdigheid van de invulling van normen. Onder andere voor het signaleren van onvolledig ingevulde normen, beoordelingen en/of beheersmaatregelen.

De Oplossing dient daarnaast functionaliteit te bieden voor het signaleren voor het (on)volledig en tijdig invullen van de normen en/of beheersmaatregelen. Validatieregels dienen binnen de standaard configuratiemogelijkheden van de Oplossing door geautoriseerde Gebruikers van Opdrachtgever, zoals functioneel beheerders, te kunnen worden ingericht of aangepast, zonder dat hiervoor maatwerkontwikkeling noodzakelijk is.

## 2.10 Contextuele ondersteuning

De Oplossing dient Gebruikers actief te ondersteunen bij het interpreteren en toepassen van normen binnen de tool. Hierbij geldt dat de Oplossing ten minste voorziet in:

- Contextafhankelijke helpteksten en toelichtingen bij normen, maatregelen en beoordelingscriteria;
- Gebruikersinstructies die de Gebruiker stapsgewijs ondersteunen bij het uitvoeren van werkzaamheden binnen de oplossing;
- Duidelijke uitleg van de betekenis, doelstelling en toepassing van normen en onderliggende vereisten.

## 2.11 Logging en monitoring

De Oplossing dient logging- en monitoringsfunctionaliteit te ondersteunen met betrekking tot toegang tot de omgeving en wijzigingen binnen de Oplossing.

Hierbij geldt dat:

- De Oplossing beschikt over volledige en raadpleegbare auditlogs waarin gebruikers-, systeem- en beheeractiviteiten worden vastgelegd;
- Auditlogs worden opgeslagen volgens het WORM-principe (Write Once, Read Many), zodat de integriteit van loggegevens is gewaarborgd en analyses op deze gegevens kunnen worden uitgevoerd;
- Auditlogs uitsluitend toegankelijk zijn voor daartoe geautoriseerde gebruikers op basis van passende autorisatie- en toegangsbeheersmaatregelen;
- Auditlogs gedurende een configureerbare of vooraf overeengekomen bewaartermijn beschikbaar blijven ten behoeve van audits, forensisch onderzoek en compliance-doeleinden. Auditlogs maken bij beëindiging van de Overeenkomst onderdeel uit van de totaalexport, zoals nader geregeld in paragraaf 3.2 (Exit data en documentatie).

## 2.12 Back-up

Opdrachtnemer dient te beschikken over gedocumenteerde en aantoonbaar geïmplementeerde back-up- en herstelprocedures voor de Oplossing.

Deze procedures dienen in ieder geval te beschrijven:

- De frequentie, reikwijdte en wijze van het maken van back-ups van gegevens en configuraties;
- De procedure voor het herstellen van gegevens en/of functionaliteiten bij verstoringen, incidenten of dataverlies;
- De periodieke controle en validatie van de werking van back-ups en herstelprocedures.

Voor de Recovery Point Objective (RPO) geldt binnen de Oplossing dat bij een verstoring maximaal vier (4) uur data verloren mag zijn.

Voor de Recovery Time Objective (RTO) geldt dat de Oplossing bij een verstoring uiterlijk binnen acht (8) uur volledig hersteld en operationeel moet zijn.

Back-ups worden op zodanige wijze opgeslagen dat deze fysiek en/of technisch gescheiden zijn van de primaire opslaglocatie, zodanig dat de back-up bij uitval van de primaire opslaglocatie of het datacenter waarin deze zich bevindt, niet verloren gaat of ontoegankelijk wordt.

## **2.13 Maatregelen**

De GRC-oplossing ondersteunt Gebruikers bij het verbeteren van de volwassenheid door per maatregel ten minste gerichte suggesties te bieden voor mogelijke verbeteracties om door te groeien naar een hoger volwassenheidsniveau, minimaal op basis van hetgeen beschreven in het Normenkader IBP-FO.

## **2.14 Risico's**

De GRC-oplossing ondersteunt het leggen van relaties tussen risico's, normen en beheersmaatregelen, waarbij de volgende koppelingen gemaakt kunnen worden:

- Eén risico aan meerdere normen;
- Meerdere beheersmaatregelen aan één risico;
- Risico's aan meerdere beheersmaatregelen.

## **2.15 Taakafhandeling**

De Oplossing ondersteunt workflow-gestuurde taakafhandeling, waarbij taken kunnen worden aangemaakt, beheerd en uitgezet naar toegewezen actiehouders/gebruikers waarbij de prioriteit, deadline, actiehouders, voortgang en status van de taak kunnen worden geregistreerd.

De Oplossing biedt de mogelijkheid om geautomatiseerde notificaties en herinneringen voor openstaande acties, taken, reviews en goedkeuringen per e-mail te versturen op basis van configureerbare workflow-stappen, termijnen of gebeurtenissen. Daarnaast ondersteunt de Oplossing het delegeren van taken aan een andere gebruiker, waarbij de verantwoordelijkheid en historie van de taak inzichtelijk blijven.

## **2.16 GRC-functionaliteiten**

De Oplossing ondersteunt minimaal de functionaliteiten zoals beschreven in dit Programma van Eisen. De genoemde functionaliteiten dienen op het moment van ingebruikname beschikbaar te zijn in de huidige, algemeen beschikbare release van de Oplossing. Functionaliteiten die uitsluitend op de roadmap staan, in ontwikkeling zijn of pas in een toekomstige release beschikbaar komen, gelden niet ter voldoening aan de beschreven functionaliteiten.

In aanvulling op de in dit Programma van Eisen beschreven functionaliteiten, ondersteunt de Oplossing de volgende functionaliteiten:

- Een register voor verwerkingen van persoonsgegevens (verwerkingsregister), waarin minimaal de in artikel 30 AVG vereiste gegevens kunnen worden vastgelegd;
- Registratie, opvolging en rapportage van incidenten waaronder datalekken;
- Het toewijzen, uitvoeren en beheren van risicoanalyses;

- Functionaliteit voor het uitvoeren, vastleggen en beheren van Pre-DPIA's en DPIA's;
- ☒ Ondersteuning van de volledige levenscyclus van beleidsvorming en beleidsbeheer;
- ☒ Het delen van documentatie en samenwerking tussen gebruikers;
- ☒ Communicatie en samenwerking tussen verschillende locaties, vestigingen en privacyfunctionarissen;
- ☒ Het aanmaken, toewijzen, beheren en monitoren van taken voor het IBP-team;
- ☒ Functionaliteit ter ondersteuning van de Functionaris Gegevensbescherming (FG);
- ☒ Ondersteuning van de registratie, afhandeling en workflow van verzoeken van betrokkenen op grond van privacywetgeving.

## 2.17 OWASP Top 10

Opdrachtnemer dient de oplossing aantoonbaar volgens security-by-design- en security-by-default principes te ontwikkelen. Daarnaast bouwt/ontwikkelt Opdrachtnemer de Oplossing met de risico's uit de OWASP Top 10, en de betreffende mitigatie daarvan, in achtneming. Opdrachtnemer voert hiertoe op eigen kosten periodiek, doch minimaal éénmaal per jaar beveiligingstesten uit. Deze verplichting staat los van en is aanvullend op de jaarlijkse, door Opdrachtgever gefinancierde penetratietest, zoals vermeld onder paragraaf 3.4.

## 3 Eisen aan de organisatie en het beheer van de oplossing

### 3.1 Beheer

Opdrachtnemer hanteert een formeel vastgelegd beleid en procedure voor het beheer van super-userrechten/ beheeraccounts die toegang geven tot de Oplossing en/of gegevens van Opdrachtgever:

- Toekenning van dergelijke rechten is uitsluitend toegestaan aan vooraf aangewezen Gebruikers, op basis van aantoonbare autorisatie door het verantwoordelijke management van Opdrachtnemer;
- Gebruik van super-userrechten wordt aantoonbaar en toereikend gelogd, zodanig dat relevante activiteiten met geprivilegieerde rechten herleidbaar zijn en periodiek geëvalueerd (minimaal halfjaarlijks);
- Voor situaties waarin noodtoegang noodzakelijk is (noodprocedure), beschikt Opdrachtnemer over een gescheiden, formeel vastgelegde noodprocedure waarbij het gebruik van noodrechten en/of noodwachtwoorden (break the glass account) wordt geregistreerd, achteraf geëvalueerd en bijstelling van rechten plaatsvindt indien noodzakelijk;
- Opdrachtgever behoudt zich het recht voor inzage te krijgen in de logging en evaluaties van het gebruik van super-user- en noodrechten.

### 3.2 Exit data en documentatie

- Bij beëindiging van de Overeenkomst wordt alle gestructureerde data en documenten van Opdrachtgever binnen de Oplossing overgedragen aan Opdrachtgever (totaalexport). Gestructureerde data worden in een gangbaar format aan Opdrachtgever ter beschikking gesteld (CSV, Excel, HTML, XML of JSON); eventueel gekoppelde documenten in hun originele formaat. Voor het beschikbaar stellen van de data zullen geen additionele kosten in rekening worden gebracht; deze werkzaamheden worden geacht te zijn inbegrepen in de reguliere exit werkzaamheden van Opdrachtnemer. Onder deze totaalexport worden uitdrukkelijk mede begrepen de auditlogs zoals bedoeld in paragraaf 2.11 (Logging en monitoring), ongeacht of deze worden aangemerkt als data van Opdrachtgever dan wel als systeemdata van de Oplossing;
- Opdrachtnemer en subverwerkers zullen na het beëindigen van de Overeenkomst en het overdragen van de data aan Opdrachtgever, de data van de systemen onder beheer van Opdrachtnemer dan wel haar subverwerkers, uiterlijk dertig (30) dagen nadat Opdrachtgever hiertoe akkoord heeft gegeven, verwijderen. Voor het verwijderen van de data zullen geen additionele kosten in rekening worden gebracht. Opdrachtnemer stuurt een bevestiging van vernietiging/verwijdering na afronding hiervan;
- Opdrachtnemer continueert tijdens de periode totdat de beëindiging van de Overeenkomst (exit) definitief is de overeengekomen dienstverlening;

- Opdrachtnemer waarschuwt en adviseert in de bespreking over de voorbereiding van de contractbeëindiging tijdig over noodzakelijke werkzaamheden en maatregelen voor de contractbeëindiging, en werkt mee aan de overgang/overdracht aan een eventuele nieuwe leverancier van een GRC-oplossing. Opdrachtnemer werpt hierbij geen barrières op die een eventuele overgang voor Opdrachtgever zonder noodzaak bemoeilijkt. Voor zover de medewerking aan de overgang verder gaat dan de reguliere exit-werkzaamheden zoals beschreven in deze paragraaf, en dit leidt tot aanvullende kosten, maakt Opdrachtnemer dit vooraf transparant kenbaar aan Opdrachtgever. Opdrachtnemer brengt deze kosten niet in rekening zonder voorafgaand schriftelijk akkoord van Opdrachtgever op de aanvullende werkzaamheden.

### 3.3 Domein-onduidelijkheid

In gevallen waarbij Opdrachtgever na de implementatie toegang- en/of gebruiksproblemen ondervindt en het onduidelijk is in welk domein dit probleem zich afspeelt, kent Opdrachtnemer een inspanningsverplichting, binnen de redelijkerwijs van Opdrachtnemer te verwachten/verlangen kaders, om gezamenlijk met Opdrachtgever tot een probleemidentificatie dan wel probleemoplossing te komen. Als naderhand blijkt dat het probleem aantoonbaar oorsprong vindt in het domein van Opdrachtnemer, zal Opdrachtnemer voor de geleverde inspanning geen kosten in rekening brengen. Ingeval het probleem aantoonbaar geen oorsprong vindt in het domein van Opdrachtnemer, maar Opdrachtnemer significante kosten heeft gemaakt bij de geleverde inspanning, is Opdrachtnemer gerechtigd hiervoor kosten in rekening te brengen bij Opdrachtgever tegen een vooraf afgesproken en/of marktconform tarief.

### 3.4 Penetratietesten

Opdrachtnemer verleent op verzoek van Opdrachtgever medewerking aan beveiligingsonderzoeken, waaronder penetratietesten (pentests), die door of namens Opdrachtgever (ook door derden, al dan niet ingezet door Opdrachtgever) worden uitgevoerd. Deze onderzoeken dienen gedurende de looptijd van de Overeenkomst minimaal één (1) keer per jaar te worden uitgevoerd ter waarborging van de informatieveiligheid van de oplossing. De kosten van dergelijke onderzoeken zijn voor rekening van Opdrachtgever.

Gedurende de pentesten wordt minimaal getoetst op de OWASP Top 10.

Opdrachtnemer informeert Opdrachtgever na afronding van een penetratietest onverwijld over de uitkomsten van het onderzoek en verstrekt daarbij ten minste een managementsamenvatting. Opdrachtnemer heeft aantoonbare procedures geïmplementeerd voor het tijdig en adequaat opvolgen en oplossen van bevindingen in zoverre naar voren gekomen gedurende de pentesten, inclusief prioritering.

### 3.5 DPIA

Opdrachtgever heeft het recht op verzoek als verwerkingsverantwoordelijke een DPIA of audit bij Opdrachtnemer uit te (laten) voeren. Opdrachtnemer werkt kosteloos en zonder opwerping van onnodige belemmeringen, binnen redelijke, in overleg vast te stellen kaders mee aan een DPIA of audit en neemt maatregelen voor zover deze daaruit voortvloeien actief op. SIVON is gerechtigd dergelijke DPIA of audit namens Opdrachtgever uit te voeren.

### 3.6 Externe communicatie

Opdrachtnemer mag uitsluitend na voorafgaande schriftelijke toestemming van Opdrachtgever extern communiceren over de inhoud of uitvoering van de Overeenkomst, dan wel de opdracht gebruiken voor commerciële uitingen, waaronder reclame, referenties, persberichten of andere publicitaire doeleinden.

### 3.7 Import

Opdrachtnemer ondersteunt op verzoek van Opdrachtgever bij de migratie en import van gegevens uit bestaande GRC-oplossingen (in geval van overstap). Deze ondersteuning omvat ten minste het analyseren van brongegevens, het in kaart brengen van gegevensstructuren en het importeren van de overeengekomen datasets in de Oplossing. Als aan deze werkzaamheden additionele kosten zijn verbonden, dient Opdrachtnemer dit vooraf kenbaar te maken bij Opdrachtgever. Opdrachtgever dient expliciet akkoord te geven op deze kosten alvorens wordt gestart met de werkzaamheden.

### 3.8 Ondersteuning

Opdrachtnemer ondersteunt Opdrachtgever passend bij de implementatie en ingebruikname van de GRC-oplossing. Daarnaast verzorgt Opdrachtnemer kennisoverdracht aan beheerders en Gebruikers van de Oplossing door middel van documentatie, handleidingen, instructiemateriaal en/of trainingen. Indien Opdrachtnemer voor deze ondersteuning meerkosten in rekening brengt, dient Opdrachtnemer dit vooraf transparant kenbaar te maken aan Opdrachtgever. Opdrachtnemer brengt deze kosten niet in rekening alvorens schriftelijk akkoord door Opdrachtgever op de gedefinieerde inzet en kosten.

## 4 Eisen aan Service Level Afspraken (SLA)

### 4.1 Supportvenster

Opdrachtnemer levert minimaal 2<sup>e</sup> en/of 3<sup>e</sup> lijnsupport aan Opdrachtgever van maandag tot en met vrijdag tussen 08.00-17.00 uur (CET), met uitzondering van officiële Nederlandse feestdagen. Opdrachtgever is zelf verantwoordelijk voor de uitvoering van 1<sup>e</sup> lijn support, tenzij anders overeengekomen tussen Opdrachtnemer en Opdrachtgever. Opdrachtnemer en Opdrachtgever komen een communicatiewijze -en kanaal aangaande de support, evenals reactie-, respons- en oplostijden overeen, welke worden vastgelegd in de Hoofdovereenkomst.

### 4.2 Onderhoud en geplande uitval

Opdrachtnemer voert updates, upgrades, patches en ander preventief onderhoud uitsluitend uit binnen een vooraf met Opdrachtgever overeengekomen onderhoudsvenster (hierbij wordt als uitgangspunt gehanteerd: ma-vr 20:00-07:00 uur en in het weekend, za-zo, tenzij hierover andere afspraken worden gemaakt). Voor noodwijzigingen (zoals vermeld onder eis 4.4.) geldt in ieder geval een uitzondering. Het geplande onderhoud inclusief verwachte duur en het effect op het gebruik wordt minimaal tien (10) werkdagen voorafgaand aan de uitvoering van het onderhoud aangekondigd aan Opdrachtgever.

Daarnaast worden Gebruikers minimaal twee (2) werkdagen voorafgaand aan het moment van gepland onderhoud adequaat geïnformeerd over het aanstaande onderhoud binnen de Oplossing, op dusdanige wijze dat alle Gebruikers hiervan tijdig kennis kunnen nemen.

### 4.3 Beschikbaarheid

De oplossing is 24x7 beschikbaar en heeft een beschikbaarheid van minimaal 99% per kalendermaand binnen kantooruren (maandag t/m vrijdag 08:00-17:00 (CET)) en minimaal 95% buiten kantooruren. De beschikbaarheid wordt vastgesteld als het percentage beschikbare minuten ten opzichte van het totale aantal minuten binnen kantooruren in de betreffende kalendermaand, waarbij vooraf aangekondigd en met Opdrachtgever afgestemd gepland onderhoud buiten beschouwing wordt gelaten. De beschikbaarheid wordt berekend volgens de formule: **(aantal beschikbare minuten/totaal aantal minuten in de kalendermaand binnen (of buiten) kantooruren, exclusief gepland onderhoud) x 100%.**

Opdrachtnemer voorziet Opdrachtgever op aanvraag van een adequaat beschikbaarheidsrapportage waarin een overzicht wordt verschaft van de beschikbaarheid van de Oplossing.

### 4.4 Noodwijzigingsprocedure

Opdrachtnemer beschikt over een formeel en gedocumenteerde noodwijzigingsprocedure met concrete toegewezen verantwoordelijkheden. Bij een noodwijziging stelt Opdrachtnemer Opdrachtgever hiervan zo spoedig mogelijk op de hoogte. Noodwijzigingen worden uitgevoerd volgens de geldende procedure en achteraf geregistreerd en geëvalueerd.

## **4.5 Incident-escalatieprocedure**

Opdrachtnemer hanteert een formeel vastgelegde incident-escalatieprocedure (inclusief escalatiecriteria) die gebaseerd is op prioriteringsniveaus. Categorisering en prioritering van incidenten vindt aantoonbaar plaats op impactanalyse met bijbehorende escalatie naar verantwoordelijken. Opdrachtgever en Opdrachtnemer komen hierover concrete afspraken overeen welke worden vastgelegd in de Hoofdovereenkomst.

## 5 Rapportage en evaluatie

### 5.1 Incidentenrapportage

Opdrachtnemer voorziet Opdrachtgever op aanvraag van een incidentenrapportage waarin een overzicht wordt verschaft van alle aangemelde incidenten. In deze rapportage staat ten minste:

- Type storing (major of minor);
- Beschrijving van de aangemelde storing;
- Beschrijving van de oorzaak en oplossing;
- Startdatum en tijdstip van het incident;
- Eerste reactie datum en tijdstip op het incident;
- Einddatum en tijdstip van het incident;
- Percentage behaalde KPI's per type storing (major/minor) volgens de SLA.

### 5.2 Voortgangsrapportage

De Oplossing dient functionaliteit te bieden waarmee geautoriseerde Gebruikers realtime inzicht kunnen verkrijgen in de voortgang van assessments, openstaande acties en de actuele status daarvan.

De Oplossing dient ten minste te voorzien in:

- Realtime dashboards en rapportages waarin de voortgang van assessments inzichtelijk wordt gemaakt;
- Inzicht in openstaande, lopende en afgeronde acties, inclusief status, verantwoordelijke en relevante termijnen;
- De mogelijkheid om de voortgang en resultaten te monitoren op verschillende organisatieniveaus;
- Rapportages waarmee de volwassenheid van de organisatie ten aanzien van de toegepaste normenkaders en beheersmaatregelen inzichtelijk wordt gemaakt;
- De mogelijkheid om rapportages te filteren, exporteren en delen met geautoriseerde gebruikers.

### 5.3 Risicorapportage

De Oplossing ondersteunt het genereren, opslaan en exporteren van risicorapportages. De rapportages bieden ten minste inzicht in geregistreerde risico's, risicoscores, beheersmaatregelen, actiepunten, eigenaarschap, status en trends, en kunnen door geautoriseerde gebruikers worden samengesteld en geraadpleegd.

### 5.4 Verwerkingsregisterrapportage

De Oplossing biedt functionaliteit voor het opstellen, filteren, genereren en exporteren van rapportages uit het verwerkingsregister. Geautoriseerde gebruikers kunnen rapportages samenstellen op basis van relevante kenmerken van verwerkingen en deze exporteren naar gangbare bestandsformaten.

## 5.5 Rapportage-sjablonen

De Oplossing ondersteunt het zelfstandig aanpassen van rapportages en deze op te slaan als herbruikbare sjablonen. Deze sjablonen kunnen op een later moment opnieuw worden gebruikt, aangepast en beheerd door geautoriseerde gebruikers.

## 5.6 Rapportage-export

De Oplossing biedt de mogelijkheid om gegenereerde rapportages te exporteren naar en op te slaan in ten minste CSV, XLSX-file, PDF- en .docx-formaat, met behoud van leesbaarheid en structuur van de rapportage-inhoud.

## 5.7 Output ten behoeve van sectorbeeld funderend onderwijs

Opdrachtnemer levert op verzoek van Opdrachtgever en/of SIVON een beveiligd en geanonimiseerd gegevensbestand ten behoeve van sectoranalyses, benchmarking en beleidsdoeleinden, in Excel-formaat en conform het in **Bijlage 1** opgenomen format, aan een door Opdrachtgever gedefinieerde derde(n). Het gegevensbestand bevat een complete dataset met de gevraagde gegevens van Opdrachtgever, waarbij ingeval Opdrachtnemer meerdere besturen binnen het Funderend Onderwijs (FO) als gebruiker van de Oplossing kent/ bedient, het gegevensbestand van Opdrachtgever in format vergelijkbaar is aan het gegevensbestand van andere klanten binnen het FO.

Opdrachtnemer verstrekt het gevraagde bestand uiterlijk binnen één (1) maand na ontvangst van een schriftelijk verzoek van Opdrachtgever. De overdracht van het bestand dient plaats te vinden via een aantoonbaar veilige en passende methode voor gegevensuitwisseling. In de regel vindt het verzoek door Opdrachtgever éénmaal (1) per jaar plaats.

Ten behoeve van de aansluiting van de te versturen data en gegevens met het gewenste bestandsformat, dient de Oplossing minimaal te voldoen aan de volgende aspecten:

- De Oplossing ondersteunt gestandaardiseerde invoervelden voor alle normen binnen de ondersteunde normenkaders, inclusief een volwassenheidsscore op een schaal van 1 tot en met 5.
- De Oplossing mag geen automatische standaard- of defaultscores toekennen aan normen of maatregelen waarvoor geen beoordeling heeft plaatsgevonden.
- Indien een norm of maatregel niet is beoordeeld, dient dit expliciet te worden geregistreerd met de statuswaarde "Niet Bekend", zodat ondubbelzinnig kan worden vastgesteld dat geen beoordeling heeft plaatsgevonden.
- De Oplossing dient naast de volwassenheidsscores 1 tot en met 5 ten minste de volgende aanvullende statuswaarden te ondersteunen:
  - Niet Bekend **(N.B.)**
  - Niet Van Toepassing **(N.V.T.)**

- De statuswaarden dienen afzonderlijk en eenduidig te worden geregistreerd en opgenomen in de geëxporteerde dataset.
- Opdrachtgever kent een unieke, persistente identificatie, waarbij deze identificatie in de tijd gelijk blijft, zodat voortgang, analyses en trends over meerdere datasets heen herleidbaar en vergelijkbaar blijven.