SIVON

Vragenlijst ten behoeve van DPIA SIVON

VERSIE 1.1 JUNI 2023

Versie beheer

Datum	Versie	Wijziging
Juni 2023	1.1	Bij deze update is er een onderscheid in de tabellen aangebracht tussen informatiebeveiliging en functionele vragen. Verder heeft er een aanscherping van de vragen plaatsgevonden. Aanpassingen doorgevoerd op het gebied van indeling en toelichting.

1 Toelichting IB- en functionele vragenlijst ten behoeve van de DPIA

Als onderdeel van het uitvoeren van een zorgvuldige DPIA maakt SIVON gebruik van een standaard vragenlijst. Deze vragenlijst is mede gericht op het concretiseren van de eis van artikel 32 AVG om 'passende technische en organisatorische maatregelen' te nemen die zijn toegesneden op de risico's die samenhangen met gebruik van de toepassing. Het hoofddoel van deze vragenlijst is om een analyse te maken van (het gebruik van) de toepassing om daarmee potentiële verwerkingsrisico's in kaart te brengen. Daarnaast brengen de antwoorden in kaart welke informatie- en beveiligingsmaatregelen er al zijn genomen.

Naam leverancier:
Ingevuld door:
Naam applicatie:
Datum:

DPIA informatiebeveiligingsvragenlijst

DPIA informatiebeveiligingsvragenlijst	Toepassing binnen <naam applicatie>
Welke derdenverklaringenover informatiebeveiliging zijn beschikbaar? • (ISO-) of andersoortige informatiebeveiligingscertificering inclusief verklaring van toepasselijkheid plus scopedocument • ISAE3402 type 2 • TPM verklaringen • Een TPM verklaring op de ROSA-certificering; Indien niet aanwezig dan het ingevulde en beargumenteerde ROSA classificatiemodel (zie vraag hieronder) • Resultaten Pentesten (onder NDA) Lever hiervan de onderliggende bewijsstukken als bijlage aan.	
ROSA Maatregelen Indien er geen TPM op het ROSA classificatiemodel aanwezig is: Graag kopie van het ingevulde ROSA classificatiemodel. Op welke manier wordt er aantoonbaar voldaan aan de baseline van maatregelen opgenomen in het Certificeringsschema informatiebeveiliging en privacy ROSA) genomen? Geef ook argumentatie hoe invulling is gegeven aan de vereiste maatregelen. Lever een beschrijving aan van deze maatregelen.	
De BIV-classificatie (beschikbaarheid, integriteit en veiligheid) is vastgesteld op basis van het ROSA certificeringsschema.	☐ Ja ☐ Nee
In plaats van het individueel beantwoorden van vragen over het ROSA classificatieschema zou een TPM verklaring opgesteld door een externe auditor ook voldoen. Zijn jullie hiertoe bereid?	☐ Ja ☐ Nee
De volgende hoog risico-verwerkingen worden binnen de applicatie toegepast: ☐ (semi-) geautomatiseerde besluitvorming ☐ algoritmen ☐ profilering ☐ big data verwerkingen ☐ nieuwe technologieën Op welke wijze en met welke (technische) middelen en methoden wordt er invulling gegeven aan de toepassing van voornoemde hoog risico-verwerkingen in de applicatie?	
Toegang 1. Op welke manier krijgen gebruikers toegang tot het gebruikte systeem (identity- en axxess management)? 2. Op welke wijze is de toegang beveiligd? 3. Wordt standaard 2FA/MFA toegepast, is deze toepassing mogelijk? 4. Welke functies zijn er om rechten en rollen te beheren? (least privilege)	
Cookies Welke cookies worden geplaatst? Welke worden er gebruikt wanneer een leerkracht/leerling gebruikt maakt van het platform?	

DPIA informatiebeveiligingsvragenlijst	Toepassing binnen <naam applicatie>
Koppelingen Geef een architectuur overzicht, zoals een architectuurschets of visualisatie, van externe toepassingen waarmee data wordt uitgewisseld. Geef een opsomming van de (meest voorkomende) applicaties waarmee gekoppeld kan worden. Op welke manier zijn de gegevens tijdens de overdracht beveiligd bij koppelingen? (denk aan beveiligde webservices en/of toepassing van end-to-end encryptie). Hoe wordt de verwerking van te veel persoonsgegevens zowel aan de verstrekkende als ontvangende kant, voorkomen?	Als bijlage toegevoegd? ☐ Ja ☐ Nee
Opslag Op welke wijze en waar wordt de data opgeslagen en beveiligd? Draait de applicatie bijvoorbeeld 'on premisse' of is er sprake van een clouddienst (bij de leverancier)? Is de data versleuteld zo ja hoe?	
Back-up en restore Zijn er duidelijke afspraken over de back-up en restore van de data en de beschikking hierover? Hoe zijn de back-ups ingeregeld en wat is het data recovery point? Denk hierbij aan: 1. Een redundant methode die real-time in veiligheidsmaatregelen voorziet. Dit betekent dat het uitvallen van een harde schijf probleemloos en direct door een andere harde schijf wordt opgevangen. 2. Een off-site read only back-up.	
Security monitoring & prevention Hoe wordt hier vorm aan gegeven? Denk aan het gebruik van beveiligingssoftware en- apparatuur. De toepassing van Managed security services zoals SOC en SIEM services.	
Beveiligd mailen Heeft het systeem mogelijkheden om beveiligd te mailen bijvoorbeeld door encryptie met wachtwoord, beperkte beschikbaarheidstermijn of het niet kunnen doorsturen of downloaden. (NTA7516 en/of UBV Veilig en Betrouwbaar e-mailverkeer').	☐ Ja ☐ Nee
Indien nog niet aanwezig, zijn er concrete plannen voor het certificeren van informatiebeveiliging. Denk aan ISO27001, ISAE3402, TPM verklaring. Zo ja op welke termijn?	☐ Ja ☐ Nee

DPIA functionele vragenlijst

DPIA functionele vragenlijst	Toepassing binnen <naam applicatie>
Privacy by default Zijn de instellingen voor de accounthouder/gebruiker 'by default' ingesteld voor alle toepassingen op de meest privacy vriendelijke instellingen?	
Privacy by design Welke privacy vriendelijke instellingen kunnen er gemaakt worden? Bijvoorbeeld in de applicatie ingebouwde waarborgen ten behoeve van de beperking van gegevensverzameling, anonimisering, transparantie, gebruikerscontrole, afschermen onnodige/optionele velden, afschermen niet afgenomen modules, mogelijkheden tot opschonen etc. Hoe wordt het principe van data-minimalisatie toegepast en welke instellingen zijn hiervoor mogelijk? Zie ook: Normenkader 8.1 Systeemontwikkeling	
Gebruikmaken rechten van betrokkenen Welke mogelijkheden zijn er t.b.v. het uitvoeren van de rechten van betrokken? (informatie, inzage, rectificatie, verwijdering, bezwaar, gegevensoverdracht + logging/statistieken, transparantie over verwerkingen (personal data & service data en telemetry data)).	
Resultaat rechten van betrokkenen Hoe werkt het proces van inzage verzoeken?	
Exportmogelijkheden Is er toegang tot bulk data middels download functie /export knop.	
Bewaartermijnen Hoe is er vormgegeven aan de bewaartermijnen waar de verwerkingsverantwoordelijke aan moet voldoen? Zijn deze standaard ingesteld, hoe zijn deze te wijzigen? Zijn er technische mechanismen, automatische verwijderprocessen en/of archiveringsmogelijkheden? Wat gebeurt er met de data in geval van beëindiging van het contract. Zijn hiervoor afspraken overeengekomen, zo ja waar? Zie ook: Normenkader 9.4 Datamanagement	
Verwijderen Hoe werkt het verwijderen van persoonsgegevens uit het systeem, bij de subverwerkers en de back-up?	

2 Toelichting loggingvragenlijst

Het belang van logging als beheersmaatregel wordt vanuit verschillende organisaties onderstreept en aan de hand van normeringen en uitgangspunten van criteria voorzien. Binnen het funderend onderwijs wordt hiervoor in het normenkader onder SM.04 (p.62) de basis gelegd.

Vastlegging van gebeurtenissen en acties in een informatiesysteem geeft inzicht in wie en wanneer bepaalde gegevens zijn bekeken of aangepast. Ook pogingen tot ongeautoriseerde toegang tot systemen, zoals ddos- of ransomware aanvallen zijn door logging herleidbaar.

De verplichting om logbestanden aan te houden en regelmatig te controleren, vormt een essentieel onderdeel van de voorschriften voor informatiebeveiliging. Logging bestaat uit functionele en technische logging.

De functionele logging dient door de school zelf gemonitord te kunnen worden, niet enkel door de leverancier. Op die manier kan een organisatie zicht houden welke medewerker wanneer en met welk doel bepaalde informatie raadpleegt of wijzigt. Het is daarnaast noodzakelijk dat er periodieke monitoring van de vastgelegde logbestanden plaatsvindt om ongebruikelijke patronen te kunnen detecteren en bijvoorbeeld te kunnen nagaan of ongeoorloofde toegang tot de gegevens plaatsvindt.

Om inzicht te krijgen in welke mate logging binnen de voorliggende applicatie is toegepast, wordt gebruikt gemaakt van onderstaande tabel. Het is aan de leverancier om deze te vullen en indien nodig van toelichting te voorzien.

Voor zover er sprake is van afwijkende logging mogelijkheden wordt verzocht deze ook in deze tabel op te nemen.

Naam leverancier:
Ingevuld door:
Naam applicatie:
Datum:

Loggingvragenlijst

Normering	Vorm van logging/monitoring	Voldaan (ja/nee)	Toelichting	Eigenaar
SM.04 Normenkader IBP (11.4)	Eisen voor logging zijn formeel vastgelegd; de procedures en toegepaste technieken voor het onderhouden, opslaan en evalueren van logging zijn gedocumenteerd, formeel vastgelegd, en gebaseerd op risicoanalyse.	☐ Ja ☐ Nee		
ROSA **Certificeringsschema informatiebeveiliging en privacy**	Logging eisen op basis van BIV-classificatie op basis van het Toetsingskader behorend bij het Certificeringsschema ROSA 3.0	BIV-classificatie (laag, midden hoog), vul in: .. / .. / ..		
	Kwaliteit logging: Er worden best practices gehanteerd zoals OWASP Logging cheat sheet	☐ Ja ☐ Nee		
	Integriteit en/of Vertrouwelijkheid			
	Laag			
	• inlogactiviteit gebruikers (toegang tot applicatie zowel gelukt als mislukt) en technisch beheer wordt gelogd en alleen gebruikt voor controle of ondersteuning (doelbinding)	☐ Ja ☐ Nee		
	• Ad hoc controle logging	☐ Ja ☐ Nee		
	• Logging is alleen toegankelijk voor bevoegde medewerkers	☐ Ja ☐ Nee		
	• Het is herleidbaar welke gegevens gewijzigd zijn.	☐ Ja ☐ Nee		

Normering	Vorm van logging/monitoring	Voldaan (ja/nee)	Toelichting	Eigenaar
	Midden			
	• inlogactiviteit gebruikers (toegang tot applicatie zowel gelukt als mislukt), lezen en wijziging van (persoons) gegevens, worden gelogd en alleen gebruikt voor controle of ondersteuning (doelbinding)	☐ Ja ☐ Nee		
	• Periodiek controle logging op afwijkende patronen (frequentie, oorsprong, et cetera)	☐ Ja ☐ Nee		
	• Logging is alleen toegankelijk voor bevoegde medewerkers	☐ Ja ☐ Nee		
	• Het is herleidbaar, wanneer, welke gegevens gewijzigd zijn.	☐ Ja ☐ Nee		
	• Wijziging van gegevens is inzichtelijk, zodat een analyse hierop mogelijk is.	☐ Ja ☐ Nee		
	Hoog			
	• inlogactiviteit gebruikers (toegang tot applicatie, zowel gelukt als mislukt) en lezen en wijziging van (persoons) gegevens worden gelogd, en alleen gebruikt voor controle of ondersteuning (doelbinding)	☐ Ja ☐ Nee		
	• Logging wordt geautomatiseerd gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera)	☐ Ja ☐ Nee		
	• Logging is op basis van autorisatie alleen toegankelijk voor relevante medewerkers	☐ Ja ☐ Nee		
	• Het is herleidbaar wie, wanneer, welke gegevens gewijzigd heeft.	☐ Ja ☐ Nee		
	• Wijziging van gegevens is inzichtelijk, waarop tevens signalering ingesteld kan worden voor bv. Ongebruikelijke transacties.	☐ Ja ☐ Nee		
	• Logging wordt geautomatiseerd gecontroleerd op afwijkende patronen (frequentie, oorsprong, et cetera)	☐ Ja ☐ Nee		
	• Logging is alleen toegankelijk voor relevante medewerkers en wordt beschermd tegen ongeautoriseerde wijzigingen.	☐ Ja ☐ Nee		
SM.04 Normenkader IBP (11.4)	De procedure is conform **business requirements**. Dit betekent o.a. dat op basis van een expliciete risicoafweging per applicatie wordt bepaald hoe lang de logging bewaard dient te worden en of er aanvullende eisen voor de logging zijn.	☐ Ja ☐ Nee		

Normering	Vorm van logging/monitoring	Voldaan (ja/nee)	Toelichting	Eigenaar
ROSA **Certificeringsschema informatiebeveiliging en privacy**	**Bewaren Logging** Gelogd wordt: inlogactiviteit gebruikers. Deze logging wordt alleen gebruikt voor controle of ondersteuning (doelbinding) en **minimaal 13 maanden** bewaard, tenzij expliciet anders is afgesproken.	☐ Ja ☐ Nee		
SM.04 Normenkader IBP (11.4)**)**	Het loggen van **ongebruikelijke activiteiten** en incorrecte of gebrekkige logging wordt gedocumenteerd, geanalyseerd en opgevolgd met gepaste maatregelen.	☐ Ja ☐ Nee		
SM.04 Normenkader IBP (11.4)	**Voorwaarden logregel** Een logregel bevat minimaal informatie over de gebeurtenis of handeling:	☐ Ja ☐ Nee		
	• Welke gebruiker deze uitvoert	☐ Ja ☐ Nee		
	• Vanaf welk apparaat dit gebeurt	☐ Ja ☐ Nee		
	• Het resultaat van de actie en een datum en tijdstip van de handeling.	☐ Ja ☐ Nee		
SM.04 Normenkader IBP (11.4)	**Systeembeheerders** Ook activiteiten van systeembeheerders worden vastgelegd in de logging.	☐ Ja ☐ Nee		
ROSA **Certificeringsschema informatiebeveiliging en privacy**	**Technisch beheer en aanpassingen** Configuratie en toepassing alsmede overige handelingen technisch beheer worden gelogd	☐ Ja ☐ Nee		
SM.04 Normenkader IBP (11.4)	**Wijzigingen in logging** Er zijn waarborgen dat de logging niet gewijzigd kan worden. Eventuele wijzigingen in logging of pogingen tot het verwijderen van logging dienen vastgelegd te worden in de logging zelf.	☐ Ja ☐ Nee		
ROSA **Certificeringsschema informatiebeveiliging en privacy**	Logging wordt beschermd tegen ongeautoriseerde wijzigingen	☐ Ja ☐ Nee		
SM.04 Normenkader IBP (11.4)	**Controle van de logging** Er vindt periodieke controle van de logging plaats om ongebruikelijke activiteiten te ontdekken. Grotere organisaties kunnen hiervoor bijvoorbeeld een SIEM (Security Incident en Event Managementsysteem) inzetten zodat automatische controle plaatsvindt.			
ROSA **Certificeringsschema informatiebeveiliging en privacy**	Logging van toegang tot logging wordt regelmatig gecontroleerd op uitzonderingen op toegang en uitzonderlijke partronen in gebruik (automatische loganalysetooling)	☐ Ja ☐ Nee		

Normering	Vorm van logging/monitoring	Voldaan (ja/nee)	Toelichting	Eigenaar
SM.04 Normenkader IBP (11.4)	**Overzicht** IT heeft een overzicht van alle logbestanden binnen de organisatie.	☐ Ja ☐ Nee		
Onderzoek van de Autoriteit Persoonsgegevens januari 2018 (landingspagina).	**Direct inzichtelijk voor de school binnen de applicatie voor periodieke controles zijn:**			
	• Foutieve inlogpogingen	☐ Ja ☐ Nee		
	• Mutaties van studieresultaten (indien van toepassing)	☐ Ja ☐ Nee		
	• Uitgevoerde imports en exports	☐ Ja ☐ Nee		
	• Periodieke controle logbestanden op indicaties onrechtmatig gebruik	☐ Ja ☐ Nee		
	Geef aan welke logging binnen de applicatie (dus zonder tussenkomst van de leverancier) direct voor de school inzichtelijk zijn. Zo nee, op welke wijze krijgen scholen dan toegang tot de logbestanden?			
	Is er specifieke audit logging voor de school (FG) beschikbaar?	☐ Ja ☐ Nee		
	Biedt de leverancier ondersteuning bij toegang tot de complete logging bijv. In geval van incidenten?	☐ toegang tot en/of verstrekking logging is altijd kosteloos		
	Algemeen: voor welke (vormen van) toegang tot logging worden (aparte/specifieke) kosten in rekening gebracht door de leverancier?	☐ Zie toelichting voor duiding		
Artikel 13 AVG	**Informatieplicht** Gebruikers worden voorafgaand aan het gebruik van het systeem geïnformeerd over de verwerking van de logginggegevens en het doel daarvan.	☐ Ja ☐ Nee		