Invitare
openbaar onderwijs

IBP beleid Invitare

‘Voluit jezelf, samen sterker’

OPGESTELD DOOR	AVG werkgroep
INSTEMMING GMR OP	7 april 2025
VASTGESTELD DOOR	CvB
VASTGESTELD OP	7 april 2025
TE EVALUEREN IN	2028/2029

Inhoudsopgave

1	**Inleiding**	**4**
1.1	Onze intentie	4
1.2	Doelstelling	4
1.3	Reikwijdte	5
2	**Juridisch kader**	**6**
2.1	Wettelijke en reglementaire kaders	6
2.2	Normen en standaarden	6
3	**Eigenaarschap en verantwoordelijkheden**	**7**
3.1	Inrichting van de governance van Invitare	7
3.2	Medezeggenschap	7
4	**Beleidsthema's informatiebeveiliging**	**8**
4.1	Risicomanagement	8
4.2	Kennis en afhankelijkheid medewerkers	9
4.3	Bedrijfscontinuïteit	9
4.4	Back-up en herstel	9
4.5	Fysieke beveiliging	9
4.6	Syteem- en data-eigenaarschap en configuratiebeheer	10
4.7	Classificatie van systemen en data	10
4.8	Securitybaseline	11
4.9	Bewustwording	11
4.10	Incident- en probleemmanagement	11
4.11	Risicomanagement leveranciers	12
4.12	Werkplekken en mobiele apparaten	12
4.13	Identiteits- en toegangsbeheer	13
4.14	Vulnerability management en pentesting	13
4.15	Patchmanagement	13
4.16	Logging	13
4.17	Digitaal sleutelbeheer	14
5	**Uitgangspunten privacy**	**15**
5.1	Persoonsgegevens	15
5.2	Privacy vuistregels	15
6	**Beleidsthema's privacy**	**18**

6.1 Verwerkingsregister 18
6.2 Informatieplicht 20
6.3 Toestemming 20
6.4 Privacy by design en privacy by default 21
6.5 Bewaartermijnen 21
6.6 Afhandelen van datalekken 21
6.7 Data Protection Impact Assessment 22
6.8 Uitwisseling persoonsgegevens 22
6.9 Rechten van betrokkenen 23

7 Verantwoording IBP 24
7.1 Naleving AVG 24
7.2 Rapportage 24
7.3 Beleidsherziening 24

1 Inleiding

Het onderwijs is in toenemende mate afhankelijk van informatie en ICT. Lesmateriaal wordt digitaal aangeboden, toetsingsprogramma's worden digitaal en de resultaten en ontwikkelingen van leerlingen worden opgenomen in een digitaal leerlingvolgsysteem. Daarnaast wordt ook veel gebruikgemaakt van digitale communicatie tussen de school, leerlingen en ouders/verzorgers. Door deze ontwikkelingen neemt het risico op verstoring van het onderwijs, verlies of misbruik van gegevens en overmatige dataverzameling toe. Het is de verantwoordelijkheid van Stichting Invitare om dat te voorkomen en een veilige leeromgeving te bieden.

Dit beleid voor informatiebeveiliging en privacy (IBP-beleid) beschrijft hoe Invitare omgaat met de beveiliging van informatie en hoe de verwerking van (persoons)gegevens wordt gewaarborgd en gehandhaafd. In het beleid worden de verschillende rollen en verantwoordelijkheden binnen Invitare op het gebied van informatiebeveiliging en privacy (IBP) beschreven.

1.1 Onze intentie

Invitare draagt de verantwoordelijkheid voor het creëren van een veilige werk- en leeromgeving. Dit houdt in dat Invitare passende technische en organisatorische maatregelen toepast om informatie te beschermen en ongeoorloofde toegang, verlies of misbruik te voorkomen.

Het recht op privacy is een grondrecht. Iedereen heeft recht op privacy en bescherming van de persoonlijke levenssfeer. Dit geldt vanzelfsprekend ook voor leerlingen, ouders/verzorgers, medewerkers en docenten. Invitare is verantwoordelijkheid voor het waarborgen van de privacy van de leerlingen en het personeel. Dit betekent ook dat deze betrokkenen zeggenschap hebben over het gebruik van hun persoonsgegevens, zoals wettelijk bepaald.

Bij Invitare staat het bieden van 'gewoon goed onderwijs' voorop. Om dit te kunnen doen verwerken wij diverse persoonsgegevens van leerlingen, ouders/verzorgers, medewerkers en docenten. Invitare vindt het belangrijk om informatie goed te beschermen en veilig en verantwoord met persoonsgegevens om te gaan. Het goed regelen van informatiebeveiliging en privacy in een beleid is noodzakelijk om de gevolgen van mogelijke informatiebeveiliging- en privacy risico's tot een aanvaardbaar niveau terug te brengen en de voortgang van het onderwijs te kunnen waarborgen.

1.2 Doelstelling

Dit IBP-beleid is erop gericht de kwaliteit van de verwerking van (persoons)gegevens en de beveiliging van informatie en systemen te verhogen. Hierbij moet een juiste balans bestaan tussen veiligheid, privacy en functionaliteit. Het uitgangspunt is dat een veilige werk- en

leeromgeving wordt gecreëerd, de persoonlijke levenssfeer van de betrokkenen wordt gerespecteerd en Invitare voldoet aan relevante wet- en regelgeving. Dit gebeurt onder andere door bewustwording te vergroten over het belang van het zorgvuldig omgaan met informatie, systemen en persoonsgegevens.

Invitare maakt gebruik van het 'Normenkader Informatiebeveiliging en Privacy voor het onderwijs' - oftewel het Normenkader IBP - om inzichtelijk te maken waar de organisatie nu staat en welke maatregelen genomen moeten worden om een veilige werkomgeving te creëren en te voldoen aan de AVG.

1.3 Reikwijdte

Dit beleid is van toepassing op alle leerlingen, docenten, medewerkers, bezoekers, ouders/verzorgers, derde partijen en andere gebruikers die toegang hebben tot of werken met de informatie van Invitare. Het beleid heeft betrekking op de verwerking van alle soorten gegevens en informatie waaronder; persoonsgegevens, bedrijfsinformatie en technische gegevens. Het is van toepassing op alle gegevensverwerkingen die onder de AVG vallen.

Informatiebeveiliging en privacy maken integraal onderdeel uit van dit IBP-beleid. Informatiebeveiliging is een belangrijke voorwaarde voor privacy. Informatiebeveiliging omvat de beveiliging van alle informatie, terwijl privacy gaat over de verwerking van persoonsgegevens.

2 Juridisch kader

2.1 Wettelijke en reglementaire kaders

Het juridisch kader voor dit IBP-beleid wordt gevormd door de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet UAVG. Daarnaast kunnen uit andere wet- en regelgeving verplichtingen of instructies voortvloeien voor de verwerking van persoonsgegevens. Voor Invitare is op dit gebied onder andere de volgende wetgeving van belang:

- Wet op het primair onderwijs (WPO)
- Wet onderwijstoezicht
- Archiefwet en archiefbesluit
- Leerplichtwet
- Wet medezeggenschap op scholen
- Arbeidsregelgeving en CAO
- Belastingwetgeving
- Telecommunicatiewet en e-privacy wetgeving

Indien een (mogelijke) strijdigheid tussen dit beleid en de AVG en/of gerelateerde wet- en regelgeving bestaat, dan moet voorafgaand aan een verwerking overlegd worden met de afdeling Juridische zaken en de privacy officer.

2.2 Normen en standaarden

De onderwijssector heeft afgesproken toe te werken naar één normenkader om aan de minimale vereisten te voldoen voor digitaal veilig onderwijs. Dit is het 'Normenkader Informatiebeveiliging en Privacy voor het onderwijs'. Dit normenkader beschrijft de regels, principes en standaarden op het gebied van informatiebeveiliging en privacy waaraan Invitare moet voldoen voor een digitale veilige schoolomgeving.

Het realiseren van het Normenkader binnen Invitare is intensieve en erg specifieke opdracht. Stichting Invitare maakt gebruik van de kennis en tools van Kennisnet en SIVON.

In dit voorliggende beleidsdocument gaan we in op de rechten van medewerkers en leerlingen en als afgeleide die van hun ouders / verzorgers. Het beleid heeft tot doel:

- De persoonlijke levenssfeer van de leerlingen en medewerkers te beschermen tegen verkeerd en onbedoeld gebruik van de persoonsgegevens;
- Vast te stellen welke persoonsgegevens de scholen en de stichting als geheel verwerken en met welk doel zij dit doen;
- De zorgvuldige verwerking van persoonsgegevens te waarborgen;
- De rechten van ouders / verzorgers, leerlingen en medewerkers inzake privacy te waarborgen.

3 Eigenaarschap en verantwoordelijkheden

3.1 Inrichting van de governance van Invitare

Informatiebeveiliging en privacy is bij Invitare ingericht volgens het 'Drie lagen model'. Het 3L-model is een leidraad bij het inrichten van de governance van een organisatie.

Eerste lijn: eindverantwoordelijkheid bij het bestuur

Invitare heeft als uitgangspunt dat de eerste lijn verantwoordelijk is voor processen, informatie en systemen van de organisatie, de risico's die hieruit voortvloeien en het treffen van de juiste maatregelen om de risico's te verkleinen. De eerste lijn bestaat uit het bestuur, directeuren en het verdere lijnmanagement van Invitare.
Het bestuur is binnen de eerste lijn eindverantwoordelijk voor informatiebeveiliging en privacy, maar kan bepaalde verantwoordelijkheden beleggen bij andere functies binnen de organisatie. Bij de beschrijving van de beleidsthema's in hoofdstuk 4 en 6 wordt per thema beschreven wie waarvoor verantwoordelijk is.

Tweede lijn: adviseren en ondersteunen

Naast de eerste lijn moet er een rol zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management de verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. De tweede lijn bestaat uit security officers, privacy officers, IBP werkgroep en juridische adviseurs.

Derde lijn: onafhankelijke controle

De derde lijn controleert of de eerste en tweede lijn soepel samenwerken en goed functioneren. De derde lijn is onafhankelijk, opereert los van de andere organisatieonderdelen en suggereert waar nodig verbeteringen.
Vanuit de MOSA groep (voor financiële en personele administratie) werken privacy officers samen en delen kennis. Daarnaast zijn alle besturen vanaf 1-1-2025 aangesloten bij een extern bureau 'Privacy op School'. PoS ondersteunt bij het realiseren van het normenkader. Vanuit deze organisatie is een externe Functionaris Gegevensbescherming (FG) gekoppeld aan elk bestuur. Deze FG heeft een wettelijke en onafhankelijke toezichthoudende taak.

3.2 Medezeggenschap

Invitare betrekt de gemeenschappelijke medezeggenschapsraad (GMR) bij besluiten over regelingen en procedures ten aanzien van bescherming van persoonsgegevens. Het schoolbestuur is eindverantwoordelijk voor het informeren van de GMR en voor het opstellen van instemmingsprocedures zoals het vaststellen van dit IBP- beleid.

4 Beleidsthema's informatiebeveiliging

Invitare gaat zorgvuldig om met de persoonsgegevens van leerlingen, hun ouders / verzorgers en medewerkers. Ze beveiligen de gegevens tegen risico's zoals verlies, onbevoegde toegang, vernietiging, gebruik, wijziging of openbaarmaking van gegevens. Via de verwerkersovereenkomsten legt Invitare deze eis ook op aan uitgevers en leveranciers.

4.1 Risicomanagement

Het risicomanagement bestaat uit een aantal stappen die er samen voor zorgen dat de risico's binnen Invitare worden beheerd. Het risicomanagementproces bestaat uit 4 stappen. We lichten hieronder de stappen toe.

4.1.1 Identificatie

Om ervoor te zorgen dat risico's worden beheerd, moeten ze in kaart zijn gebracht. De eerste lijn is verantwoordelijk voor het identificeren van risico's die mogelijk een negatieve impact hebben op de doelstellingen van het betreffende organisatieonderdeel. Het schoolbestuur en de scholen die eronder vallen hebben de gezamenlijke verantwoordelijkheid voor het identificeren van risico's die betrekking hebben op de gehele organisatie. De verantwoordelijkheid voor het registreren van risico's is belegd in de eerste lijn.

4.1.2 Analyse

De kans en impact van een risico worden aan de hand van periodieke risicoanalyses bepaald. Invitare is aangesloten bij Your Safety Net (YSN). Het realiseren van het normenkader IBP is groot en tijdrovend. De tools van YSN ondersteunen en het systeem biedt voorbeeldteksten en sjablonen voor een stevige IBP-basis.
In januari 2025 heeft een 0-meting voor onze Stichting plaats gevonden aan de hand van het instrument van YSN. Het resultaat van de 0-meting is uitgangspunt in het verder uitzetten van de nodige IBP activiteiten.

4.1.3 Beheersing

Aan de hand van de 0-meting stellen we een tijdpad op tot 2027. We gaan er hierbij vanuit in 2027 het volwassenheidsniveau 3 te behalen (zie Kennisnet).
De IBP werkgroep maakt beheerskeuzes en verdeelt de taken op basis van kennis, haalbaarheid en stelt een (meer)jaarplanning op.

4.1.4 Monitoring en rapportage

De werkgroep monitort en rapporteert vierjaarlijks aan het schoolbestuur.

4.2 Kennis en afhankelijkheid medewerkers

Invitare is voor de beveiliging van informatie en de continuïteit van het onderwijs afhankelijk van de kennis en beschikbaarheid van medewerkers. Invitare wil voorkomen dat onvoldoende kennis aanwezig is bij medewerkers of dat kritieke kennis en vaardigheden onvoldoende aanwezig zijn binnen de organisatie. Taken van sleutelfiguren moeten daarom altijd overgenomen kunnen worden door andere medewerkers. Hiervoor hanteert Invitare de volgende maatregelen:

- Voldoende training en certificering (in samenwerking met HR)
- Een indienst-/uitdiensttredingproces waarin rekening gehouden wordt met aansluiting op het proces voor het beheren van rechten en rollen, de overdracht van kennis en documentatie en screening van medewerkers (in samenwerking met IPOS en administratief medewerker).

Actie uit te voeren: updaten; in- en uitdiensttredingsprocessen

4.3 Bedrijfscontinuïteit

Invitare zorgt ervoor dat mogelijke verstoringen van het onderwijs zo snel mogelijk verholpen worden en dat de impact van verstoringen beperkt blijft. Door processen te analyseren worden de meest kritieke applicaties en medewerkers geïdentificeerd en wordt bepaald welke terugvaloptie nu aanwezig is. Hierna kunnen maatregelen geïmplementeerd worden om verstoringen zo veel mogelijk te voorkomen of de impact te beperken. De medewerkers van de ICT-afdeling in samenwerking met de externe ICT partners bewaken en monitoren periodiek de diverse systemen.

4.4 Back-up en herstel

Invitare maakt (nog) geen gebruik van back-up. Invitare gebruikt via Microsoft gebruik van retentie. Via retentie wordt data voor bepaalde tijd bewaard. De ICT afdeling is systeemeigenaar en verantwoordelijk voor het toepassen van het back-up en herstel proces.
Actie uit te voeren: realiseren voor aug. 2027; onderzoeken of back-up wenselijk is.

4.5 Fysieke beveiliging

Als instelling die zich inzet voor een veilige werk- en leeromgeving, erkennen we het belang van het identificeren, analyseren en beheersen van potentiële risico's die de continuïteit van activiteiten en de reputatie van Invitare kunnen beïnvloeden. Dit risicomanagementbeleid is nodig voor het effectief beheren van risico's. Door risico's proactief aan te pakken, proberen we negatieve gevolgen te minimaliseren en bij te dragen aan de doelstellingen die Invitare nastreeft;

- proactief identificeren van risico's en bepalen welke van invloed zijn op de doelstellingen;

- bevorderen van een cultuur van risicobewustzijn en -verantwoordelijkheid binnen de school, waarin alle leerlingen en medewerkers bijdragen aan het identificeren en beheren van risico's;
- ontwikkelen van effectieve strategieën en maatregelen om risico's te beheersen en te verminderen;
- waarborgen van de betrokkenheid van belanghebbenden door effectieve communicatie en rapportage over risico's en risicobeheersactiviteiten;
- aanpassen aan veranderende omstandigheden en nieuwe risico's.
- voldoen aan relevante wet- en regelgeving en normen met betrekking tot risicomanagement.

4.6 Syteem- en data-eigenaarschap en configuratiebeheer

Om IT-processen te beheren is inzicht nodig in welke systemen worden gebruikt binnen de organisatie. Veel van de IBP-thema's in dit beleid zijn afhankelijk van dit inzicht. De rol van systeemeigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die specifiek voor een systeem gelden. De rol van proceseigenaar wordt gebruikt om bepaalde verantwoordelijkheden toe te kunnen wijzen die te maken hebben met een specifiek proces. Invitare maakt de keuze om eigenaarschap van data niet vast te leggen, maar zich te beperken tot het beleggen van eigenaarschap van systemen waar deze data in is vastgelegd. Voor het vastleggen van processen en het eigenaarschap van systemen en processen treft Invitare de volgende maatregelen:

- Invitare heeft een configuratiemanagementdatabase (CMDB) waarin alle systemen, het eigenaarschap en andere benodigde eigenschappen bijgehouden worden.
- Systeemeigenaarschap wordt bepaald vóór implementatie van nieuwe systemen. De eigenaren van systemen worden vastgelegd in het CMDB.
- Proceseigenaarschap wordt bepaald en vastgelegd binnen het verwerkingsregister.

Actie uit te voeren: realiseren voor aug. 2027; configuratiemanagementdatabase

4.7 Classificatie van systemen en data

Om risico gestuurd beslissingen te kunnen nemen is het van belang om per systeem het benodigde niveau van beschikbaarheid, integriteit en vertrouwelijkheid (BIV) te bepalen. De classificatie is beperkt tot systeemniveau. Invitare kiest ervoor om de classificatie niet per individueel dataobject toe te passen. Invitare heeft voor elk systeem dat opgenomen is in de CMDB een BIV-classificatie uitgevoerd. Deze BIV-classificatie wordt gebruikt om te bepalen welke maatregelen er voor het betreffende systeem geïmplementeerd moeten worden. Voor het goed toepassen van de BIV-classificatie treft Invitare de volgende maatregelen:

- De BIV-classificatie wordt uitgevoerd vóór de aanschaf van een nieuw systeem. Zie beleidsthema 4.11.
- De BIV-classificatie wordt vastgelegd in de CMDB.

Actie uit te voeren: realiseren voor aug. 2027; BIV classificatie

4.8 Securitybaseline

Een securitybaseline voor IT-systemen is vastgesteld om het risico van ongeoorloofde toegang tot IT-middelen te beperken. Invitare maakt gebruik van het certificeringsschema ROSA als securitybaseline voor IT-systemen in eigen beheer. De securitybaseline is formeel vastgelegd, wordt periodiek geactualiseerd en wordt goedgekeurd door het schoolbestuur. De toepassing van de securitybaseline voor IT-middelen wordt periodiek beoordeeld op naleving. Afwijkingen van de baselines zijn gedocumenteerd en goedgekeurd.
De bestuurder is verantwoordelijk voor het formeel goedkeuren van de securitybaseline. De systeemeigenaar van elk systeem is verantwoordelijk voor het voldoen aan de securitybaseline en het vastleggen van afwijkingen op de baseline.
Actie uit te voeren: realiseren voor aug. 2027; certificeringsschema

4.9 Bewustwording

Beleid en technische maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging en privacy uit te sluiten. De mens is hierin ook een belangrijke factor. Daarom wordt het bewustzijn van medewerkers over de verantwoordelijkheden die ze hebben voortdurend aangescherpt, zodat de kennis van bestaande risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Hiervoor neemt Invitare de volgende maatregelen:

- Er zijn bewustwordingsactiviteiten die jaarlijks uitgevoerd worden zoals de schoolbezoeken met controles, fishing campagnes en diverse schriftelijke en mondelinge informatie.

De privacy officer in samenspraak met de IBP werkgroep is verantwoordelijk voor het opstellen en het beheren van het bewustwordingsactiviteiten.

4.10 Incident- en probleemmanagement

Incidentmanagement is het proces voor het melden van incidenten binnen de organisatie. Sommige incidenten kunnen een datalek tot gevolg hebben. Incidenten binnen de organisatie zijn nooit helemaal uit te sluiten. Een helder beschreven incidentmanagementproces is aanwezig om incidenten op tijd te herkennen en ze adequaat af te handelen. De manier waarop dat gebeurt is vastgelegd in een procesbeschrijving waarbij de volgende onderwerpen minimaal terugkomen:

- Een centraal punt voor het melden van incidenten.
- Incidentenregister: Binnen dit incidentenregister wordt er duidelijk onderscheid gemaakt tussen datalekken en andere type incidenten.
- De classificatie van incidenten: Bij elk incident moet worden vastgesteld om wat voor type incident het gaat (beveiliging, privacy, etc.)
- De afhandeling van het incident: Het is duidelijk wie bij welk type incident betrokken moeten worden en wie verantwoordelijk is voor het afhandelen van de incidenten.

Monitoren en rapporteren: Afhandeling van incidenten en problemen worden gemonitord. Hierover wordt periodiek gerapporteerd naar het schoolbestuur. De externe FG'er is verantwoordelijk voor het formeel goedkeuren van de incidentmanagemenprocesbeschrijving.

De privacy officer is verantwoordelijk voor het opstellen en het beheren van de incidentmanagementprocesbeschrijving en is verantwoordelijk voor het inrichten en beheren van het incidentenregister.
Actie uit te voeren: realiseren; incidentmanagementprocesbeschrijving

4.11 Risicomanagement leveranciers

Invitare besteedt een deel van de IT uit aan leveranciers, maar blijft eindverantwoordelijk voor beveiliging van informatie en persoonsgegevens. Om ervoor te zorgen dat ook leveranciers zich houden aan de technische maatregelen die volgen uit de securitybaseline zijn bepaalde stappen toegevoegd aan het leveranciersmanagementproces.
Op basis van de securitybaseline is een lijst met maatregelen opgesteld. Er is een leveranciersmanagementproces waar de volgende stappen onderdeel van zijn:

- Voor de aanschaf van een nieuw systeem wordt een BIV-classificatie uitgevoerd.
- Op basis van deze BIV-classificatie (beschikbaarheid, integriteit, vertrouwelijkheid) en de lijst met maatregelen worden aanbestedingseisen opgesteld.
- Periodiek wordt een controle gedaan op het voldoen aan de aanbestedingseisen.

De bestuurder is verantwoordelijk voor het formeel goedkeuren van de leveranciersmanagementprocesbeschrijving. De privacy officer is verantwoordelijk voor het opstellen en het beheren van de leveranciersmanagementprocesbeschrijving.
De systeemeigenaar is verantwoordelijk voor de periodieke controle op het voldoen aan de aanbestedingseisen.
Actie uit te voeren: realiseren voor aug. 2027; leveranciersmanagementprocesbeschrijving

4.12 Werkplekken en mobiele apparaten

Persoonsgegevens en andere informatie uit systemen die binnen onze organisatie worden gebruikt, worden ontsloten via verschillende apparaten zoals laptops, tablets, smartphones en desktop-pc's. Deze apparaten brengen risico's met zich mee op het gebied van beveiliging, dataverlies en compliance (naleven wet- en regelgeving). Daarom maakt Invitare gebruik van een richtlijn voor het gebruik van werkplekken en mobiele apparaten.
De bestuurder is verantwoordelijk voor het formeel goedkeuren van de richtlijn voor het gebruik van werkplekken en mobiele apparaten.
De privacy officer is verantwoordelijk voor het opstellen en het beheren van de richtlijn voor het gebruik van werkplekken en mobiele apparaten.
Actie uit te voeren: realiseren voor aug. 2027; richtlijn gebruik werkplekken/mobiele apparaten

4.13 Identiteits- en toegangsbeheer

Identity- en accessmanagement (IAM) – ook wel identiteits- en toegangsbeheer genoemd – zorgt voor het beheren van de logische toegang tot informatie, informatiediensten en externe koppelingen. Met logische toegang wordt de toegang tot systemen bedoeld. Het gaat hierbij onder andere om beleid rondom toegangsrechten, functiescheiding en super-userrechten om de informatie van Invitare, medewerkers en leerlingen te beveiligen tegen ongeoorloofde toegang.

Actie uit te voeren: realiseren voor aug. 2027; proces toegangsrechten beschrijven

4.14 Vulnerability management en pentesting

Vulnerability management (kwestbaarhedenonderzoek) en pentesting vormen een essentieel onderdeel voor het verminderen van risico's, het voorkomen van ongeautoriseerde toegang tot IT-systemen en het beschermen van gegeven tegen mogelijke dreigingen.

Actie uit te voeren: realiseren voor aug. 2027; kwetsbaarheden onderzoek

4.15 Patchmanagement

Met patchmanagement verhelp je kwetsbaarheden in systemen, applicaties en hardware. Het doel is om de beveiliging, stabiliteit en prestaties van IT-omgevingen te waarborgen door het tijdig testen en implementeren van patches. Hiervoor neemt Invitare de volgende maatregel:

- Invitare heeft een proces voor het inrichten van patchmanagement.

De bestuurder is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving patchmanagement.

De ICT medewerker is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving patchmanagement. De systeemeigenaar is verantwoordelijk voor tijdig testen en implementeren van patches.

Actie uit te voeren: realiseren voor aug. 2027; kwetsbaarhedenonderzoek voor systemen, applicaties en hardware.

4.16 Logging

Loggegevens bieden inzicht in de activiteiten van systemen en spelen een sleutelrol bij het detecteren, onderzoeken en voorkomen van beveiligingsincidenten. Om loggegevens vast te leggen neemt Invitare de volgende maatregel:

Invitare heeft een procesbeschrijving voor het vastleggen van loggegevens binnen systemen.

De bestuurder is verantwoordelijk voor het formeel goedkeuren van de procesbeschrijving voor logging.

De systeembeheerder is verantwoordelijk voor het opstellen en het beheren van de procesbeschrijving voor logging.

Actie uit te voeren: realiseren voor aug. 2027; procesbeschrijving loggegevens

4.17 Digitaal sleutelbeheer

Invitare geeft aan of de organisatie zelf cryptografische sleutels (gegevens die nodig zijn om een versleutelde boodschap te versleutelen) beheert en hoe er mee omgegaan wordt.
Actie uit te voeren: realiseren voor aug. 2027; proces beheer cryptografische sleutels

5 Uitgangspunten privacy

Het algemene uitgangspunt in dit IBP-beleid is dat persoonsgegevens in overeenstemming met de AVG en gerelateerde wet- en regelgeving op zorgvuldige wijze worden verwerkt. Om aan dit uitgangspunt te voldoen verwerkt Invitare persoonsgegevens in overeenstemming met de privacyvuistregels die verderop in dit hoofdstuk worden uiteengezet. Invitare treft verdiepende maatregelen om de beleidsthema's in dit IBP-beleid in te vullen.

5.1 Persoonsgegevens

Persoonsgegevens zijn gegevens die direct of indirect over iemand gaan en dus naar een persoon te herleiden zijn, zoals een naam of e-mailadres. Naast gewone persoonsgegevens - denk aan contactgegevens en onderwijsnummers - onderscheidt de AVG bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens. Daarnaast bestaat een categorie 'gevoelige' persoonsgegevens die niet expliciet in de AVG is benoemd. Dit zijn persoonsgegevens die vanwege hun aard privacygevoelig zijn en daarom extra bescherming verdienen.

- Bijzondere persoonsgegevens zijn gegevens die te maken hebben met bijvoorbeeld ras of etnische afkomst, gezondheid, religie of seksueel gedrag. De verwerking van deze gegevens is verboden, tenzij een wettelijke uitzondering bestaat zoals toestemming van de betrokkene.
- Strafrechtelijke gegevens zijn gegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten. De verwerking van deze gegevens is ook verboden, tenzij hiervoor een wettelijke uitzondering geldt.
- Gevoelige persoonsgegevens zijn gegevens die een groter privacyrisico vormen dan gewone persoonsgegevens. Denk aan financiële gegevens, burgerservicenummers (BSN), beoordelingen of gegevens van kwetsbare leerlingen.

NB: Nummers ter identificatie van een persoon, zoals het BSN, mogen alleen worden gebruikt voor specifieke doeleinden die in de wet zijn vastgelegd. Een onderwijsnummer (persoonsgebonden nummer) is gelijk aan het BSN.

5.2 Privacy vuistregels

Bij het verwerken van persoonsgegevens houdt Invitare rekening met onderstaande vuistregels. Door deze basisprincipes te volgen zorgen we ervoor dat we kunnen voldoen aan de AVG.

5.2.1 We verwerken persoonsgegevens rechtmatig en transparant

Invitare verzamelt en gebruikt persoonsgegevens op een eerlijke en transparante manier. Persoonsgegevens worden alleen verwerkt als daarvoor een wettelijke grondslag bestaat in de

AVG. We leggen altijd duidelijk uit waarom we bepaalde gegevens nodig hebben, wat we ermee doen en hoe lang we deze gegevens bewaren. Daarom informeren we ouders en leerlingen tijdig over het gebruik van hun persoonsgegevens, via een transparante privacyverklaring. Dit gebeurt bijvoorbeeld op het moment van inschrijving van een leerling.

5.2.2 We verwerken persoonsgegevens voor specifieke doeleinden

Invitare verwerkt persoonsgegevens alleen wanneer vooraf de specifieke doeleinden voor de verwerking zijn bepaald. Deze doeleinden worden vastgelegd. Persoonsgegevens worden niet voor andere, niet-verenigbare, doelen verwerkt. We zullen dus geen persoonsgegevens verzamelen omdat die wellicht ooit van pas gaan komen. We doen dit alleen met vooraf bepaalde, duidelijke en gerechtvaardigde doelen, zoals het plannen van onderwijs en communiceren met leerlingen en ouders over de voortgang en schoolactiviteiten.

5.2.3 We verwerken alleen noodzakelijke persoonsgegevens

Invitare verzamelt alleen persoonsgegevens die noodzakelijk zijn voor het doel waarvoor ze worden verwerkt. We vragen dus niet om meer gegevens dan we daadwerkelijk nodig hebben en hanteren hierbij het uitgangspunt 'zo min mogelijk'. We onderzoeken altijd of we met minder gegevens of enkel met anonieme gegevens kunnen werken. Zo vragen we bij de inschrijving van een leerling alleen om de gegevens die relevant zijn voor het kunnen bieden van onderwijs en bewaren we geen overbodige gegevens die niet nodig zijn voor onze schoolactiviteiten.

5.2.4 We zorgen dat persoonsgegevens juist en actueel zijn

Invitare treft maatregelen om ervoor te zorgen dat persoonsgegevens correct en actueel zijn. Onjuiste of achterhaalde gegevens worden geactualiseerd of verwijderd. Leerlingen en ouders kunnen op een laagdrempelige manier doorgeven dat persoonsgegevens incorrect zijn en/of gewijzigd moeten worden. Onze processen en systemen worden zo ingericht dat de juistheid van gegevens zoveel mogelijk wordt afgedwongen en gecontroleerd.

5.2.5 We zorgen voor een passende bescherming van persoonsgegevens

We kunnen de privacy van leerlingen, ouders en medewerkers alleen goed beschermen als we op een veilige manier met hun persoonsgegevens omgaan. We zijn daarom verantwoordelijk voor het treffen van passende technische en organisatorische beveiligingsmaatregelen. Die maatregelen moeten ervoor zorgen dat de persoonsgegevens op een passende wijze worden beveiligd en worden beschermd tegen verlies, vernietiging, beschadiging of onrechtmatige verwerking. Dit doen we bijvoorbeeld door het gebruik van veilige systemen voor de opslag van leerling gegevens en het opleiden van personeel in het veilig omgaan met gevoelige gegevens.

5.2.6 We kunnen aantonen dat we voldoen aan de AVG

We zijn verantwoordelijk voor het naleven van bovengenoemde vuistregels en kunnen daarmee aantonen dat we voldoen aan de belangrijkste uitgangspunten van de AVG. Dit doen we bijvoorbeeld door het bijhouden van een verwerkingsregister en het uitvoeren van Data Protection Impact Assesments (DPIA's) voor gegevensverwerkingen met een hoog privacyrisico.

5.2.7 We kunnen ons ethisch verantwoorden

Bij het beoordelen van verwerkingen van persoonsgegevens houdt niet alleen rekening met de vereisten uit de AVG ('mogen we dit?'), maar nadrukkelijk ook met ethische aspecten ('willen we dit?). Het gaat hierbij dus niet om de vraag of we iets 'mogen' of 'kunnen', maar juist om de vraag of we iets zouden moeten 'willen' als school.
Ethische aspecten spelen in het bijzonder een rol bij verwerkingen die privacyrisico's kunnen opleveren, bijvoorbeeld bij het gebruik van meekijksoftware of schermcontroles. Dit moet ook worden bezien vanuit een ethisch afwegingskader. We stellen ons dan ook eerst de vraag of we het kunnen uitleggen aan leerlingen en ouders.

6 Beleidsthema's privacy

6.1 Verwerkingsregister

Invitare heeft maatregelen getroffen om aantoonbaar te voldoen aan de eisen uit de AVG. Dit houdt onder meer in dat Invitare kan aantonen dat de verwerking van persoonsgegevens voldoet aan de uitgangspunten uit de AVG. Invitare geeft onder meer invulling aan haar verantwoordingsplicht door een overzicht bij te houden met informatie over de persoonsgegevens die zij verwerkt. Dit heet het verwerkingsregister. Dit register bevat bijvoorbeeld informatie over de leerlingenadministratie of het HR-systeem. Het bijhouden van het verwerkingsregister zorgt voor een goed overzicht van welke persoonsgegevens worden verwerkt en met welk doel dit gebeurt. Het register stelt Invitare in staat te voldoen aan haar verantwoordingsplicht.

Het verwerkingsregister bevat van afzonderlijke verwerkingsactiviteiten informatie over onder meer de doeleinden voor de verwerking, de toepasselijke grondslag onder de AVG, een beschrijving van de betrokkenen, een beschrijving van de persoonsgegevens, de toepasselijke bewaartermijnen en de ontvangers waarmee persoonsgegevens worden gedeeld.

6.1.1 Legitiem doel en doelbinding

Persoonsgegevens worden alleen verwerkt als een specifiek, vooraf bepaald doel is vastgesteld door Invitare. Dit doel moet duidelijk en in begrijpelijke taal aan de betrokkenen worden uitgelegd. Persoonsgegevens mogen niet voor andere doeleinden worden gebruikt.

Invitare verwerkt persoonsgegevens om haar verplichtingen als onderwijsinstelling na te kunnen komen. Het schoolbestuur verwerkt persoonsgegevens in de eerste plaats om onderwijs te kunnen bieden aan haar leerlingen en om activiteiten die hieraan ondersteunend zijn te kunnen uitvoeren. Hierbij valt te denken aan verwerkingen in het kader van het aanmeldproces, om te communiceren met leerlingen en ouders/verzorgers, het bijhouden van de leerlingenadministratie, het maken van roosters en om de voortgang bij te houden.

Ook verwerkt het schoolbestuur persoonsgegevens van haar medewerkers in haar rol als werkgever. Invitare verwerkt bij deze werkzaamheden verschillende (categorieën) persoonsgegevens, waaronder contactgegevens, naam, geboortedatum en gegevens betreffende de aard en het verloop van het onderwijs. Invitare verwerkt deze persoonsgegevens op basis van grondslagen uit de AVG, bijvoorbeeld omdat sprake is van een wettelijke taak of verplichting, een gerechtvaardigd belang of op basis van toestemming.

Als gegevens toch voor een ander doel nodig zijn, dan mag dit alleen als dat doel verenigbaar is met het oorspronkelijke doel. Om te bepalen of dit het geval is, moet onder andere worden gekeken naar:

- De relatie tussen het nieuwe en het oorspronkelijke doel.
- De context waarin de gegevens zijn verzameld en de redelijke verwachtingen van de betrokkenen.
- Het soort persoonsgegevens; gevoelige gegevens verdienen extra bescherming.
- De mogelijke gevolgen voor betrokkenen.
- Bescherming van de gegevens, zoals versleuteling of pseudonimiseren.

Voor elke nieuwe verwerking moet Invitare de rechtmatigheid, zorgvuldigheid en noodzaak opnieuw beoordelen. De specifieke doeleinden worden voorafgaand aan de verwerking bepaald en vermeld in de privacyverklaring om betrokken te informeren. Ook worden de doeleinden opgenomen in het verwerkingsregister. Voordat gegevens voor een ander doel worden gebruikt, vindt overleg plaats met de privacy officer en indien nodig ook met de functionaris gegevensbescherming.

6.1.2 Grondslag

Invitare moet voor iedere verwerking van persoonsgegevens een geldige reden hebben. De AVG noemt dit een grondslag. Invitare verwerkt persoonsgegevens alleen op basis van de in de AVG genoemde grondslagen:

- De betrokkene heeft toestemming verleend, bijvoorbeeld voor het maken en delen van foto's of video's.
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, bijvoorbeeld het verwerken van salaris om de arbeidsovereenkomst met werknemers na te komen.
- De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting, bijvoorbeeld het delen van salarisinformatie met de Belastingdienst voor de uitvoering van de belastingwetgeving.
- De verwerking is noodzakelijk om de vitale belangen van de betrokkene te beschermen, bijvoorbeeld bij een levensbedreigende situatie waarbij het noodzakelijk is dat bepaalde gegevens van een leerling acuut aan hulpverleners moeten worden doorgeven.
- De verwerking is noodzakelijk om uitvoering te geven aan een taak van algemeen belang, hierbij gaat het om wettelijk vastgestelde taken en bevoegdheden. Zo heeft Invitare de wettelijke taak om onderwijs te bieden.
- De verwerking is noodzakelijk voor de behartiging van een gerechtvaardigd belang van Invitare of van een derde. Denk hierbij aan het verwerken van medewerkersgegevens voor het opstellen van managementrapportages ten behoeve van beleidsontwikkeling of het gebruik van bewakingscamera's op het schoolplein.

De toepasselijke grondslag wordt vooraf vastgesteld, bijvoorbeeld middels een DPIA, en benoemd in de privacyverklaring om betrokken te informeren. Ook wordt de toepasselijke grondslag opgenomen in het verwerkingsregister.

6.2 Informatieplicht

Invitare verwerkt persoonsgegevens op een behoorlijke en transparantie manier. Dit is in begrijpelijke taal inzichtelijk voor de betrokkenen. Invitare informeert leerlingen, ouders en medewerkers voorafgaand aan de gegevensverwerking op transparante wijze via een duidelijke privacyverklaring. Deze privacyverklaring wordt gepubliceerd op de website. Daarnaast informeert de school medewerkers en sollicitanten ook via een aparte privacyverklaring. Hiermee zorgt Invitare ervoor dat betrokkenen weten welke persoonsgegevens worden verwerkt en voor welke doeleinden dit gebeurt. Ook zijn ze op de hoogte van de rechten die ze hebben.
Wordt gebruikt gemaakt van geautomatiseerde besluitvorming of profilering? Dan gelden extra strenge regels, ook op het gebied van transparantie. Dat betekent onder andere dat medewerkers en leerlingen goed moeten worden geïnformeerd over het gebruik hiervan en duidelijk moet worden uitgelegd op basis van welke criteria het besluit tot stand is gekomen. Ook moet de mogelijkheid bestaan een nieuw besluit te nemen waarbij een mens de gegevens beoordeelt. Op die manier beschermen we medewerkers en leerlingen tegen onrechtmatige verwerking.

6.3 Toestemming

Bij het gebruik van toestemming als grondslag gelden een aantal voorwaarden:

- Toestemming moet op een begrijpelijke en toegankelijke manier worden gevraagd, in duidelijke taal en niet verborgen in algemene voorwaarden of lange teksten.
- Toestemming moet vrijwillig worden gegeven en moet ook weer gemakkelijk ingetrokken kunnen worden.
- Invitare moet kunnen aantonen dat toestemming is verkregen, bijvoorbeeld door logs of ondertekende formulieren.
- Voor kinderen onder de 16 jaar moet een wettelijke vertegenwoordiger toestemming geven. Dit geldt ook voor personen onder curatele, bewind of mentorschap. Invitare verifieert of deze vertegenwoordiger daadwerkelijk toestemming heeft gegeven.

Leerlingen (of hun wettelijke vertegenwoordigers) worden in bepaalde situaties om toestemming gevraagd. Denk aan de situatie dat de scholen foto's of video's van leerlingen maken en publiceren.
Dit mag alleen als de school vooraf toestemming heeft verkregen. Omdat een gezagsrelatie bestaat tussen Invitare en haar leerlingen en medewerkers, moet goed worden beargumenteerd waarom toestemming in specifieke gevallen in vrijheid kan worden gegeven. Invitare gaat daarom terughoudend om met het gebruik van deze grondslag. Voordat toestemming als grondslag wordt gebruikt, vindt overleg plaats met de privacy officer en indien nodig ook met de functionaris gegevensbescherming.

6.4 Privacy by design en privacy by default

Privacy by design betekent dat Invitare bij de ontwikkeling, het ontwerp, de selectie en het gebruik van toepassingen, diensten en producten zo vroeg mogelijk rekening houdt met privacyrisico's en passende waarborgen inbouwt om de privacy van betrokkenen te beschermen. Neemt Invitare bijvoorbeeld een leerlingvolgsysteem in gebruik? Dan moet in een vroeg stadium al worden nagedacht over passende toegangsbeperkingen. Leraren horen alleen inzicht te krijgen in de noodzakelijke gegevens van hun eigen leerlingen. Privacy by default betekent dat de standaardinstellingen van een product, dienst of proces op de meest privacyvriendelijke instelling staan.

Hiermee zorgt Invitare ervoor dat zo vroeg mogelijk rekening wordt gehouden met privacybeginselen en op die manier privacyrisico's tijdig worden verkleind.

6.4.1 Dataminimalisatie

Invitare verzamelt alleen gegevens die noodzakelijk zijn voor het doel dat voorafgaand aan de verwerking is vastgesteld. De verzamelde gegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn. Hiermee voorkomt Invitare dat te veel gegevens worden verwerkt.
Bij de aanmelding van een leerling verzamelt Invitare bijvoorbeeld alleen de informatie die nodig is om de leerling op de juiste manier in te schrijven. Denk aan naam, geboortedatum, adres en contactgegevens van ouders/verzorgers. Extra informatie, zoals het beroep van de ouders, is niet relevant voor de inschrijving en hoort daarom niet te worden verzameld. Daarnaast moet de verwerking van persoonsgegevens op de minst ingrijpende wijze plaatsvinden. Als het beoogde doel op een privacyvriendelijkere manier kan worden bereikt, dan kiest Invitare hiervoor. Op deze manier voldoet Invitare eveneens aan de principes van privacy by design.

6.5 Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk voor de doeleinden waarvoor zij zijn verzameld. Dit gebeurt in overeenstemming met het bewaar- en vernietigingsbeleid van Invitare.
Na het verlopen van de toepasselijke bewaartermijnen zorgt Invitare ervoor dat persoonsgegevens tijdig worden vernietigd (of geanonimiseerd). Hierdoor worden persoonsgegevens beter beschermd tegen onnodige verwerking en datalekken. Zo worden bijvoorbeeld overzichten van schoolprestaties en rapporten uiterlijk tot 2 jaar na uitschrijving van een leerling bewaard. Het schooladvies wordt tot uiterlijk 5 jaar na uitschrijving van een leerling bewaard.

6.6 Afhandelen van datalekken

Invitare heeft vanuit de AVG heb je de verplichting datalekken adequaat en tijdig af te handelen. In de procedure datalekken beschrijf je hoe je dat doet.

Voorbeelden van datalekken zijn een gestolen laptop, een verloren usb-stick, of een e-mail met persoonsgegevens die naar de verkeerde persoon is verstuurd. Datalekken moeten direct worden gemeld via het contactpunt van Invitare dat vermeld staat op de website en geregistreerd in het interne register voor beveiligingsincidenten en datalekken. Risicovolle datalekken moeten worden gemeld aan de Autoriteit Persoonsgegevens en ook aan de betrokkenen als het datalek waarschijnlijk een hoog risico voor hen oplevert. De privacy officer beoordeelt of zo'n melding nodig is. Dit gebeurt als het nodig is in samenspraak met de functionaris gegevensbescherming.
Actie uit te voeren: realiseren voor aug. 2027; procedure datatlekken updaten

6.7 Data Protection Impact Assessment

Voor elke nieuwe verwerking van persoonsgegevens, bijvoorbeeld een nieuw proces, technologie of applicatie, controleert Invitare of de privacybeginselen uit de AVG worden nageleefd.
Bij verwerkingen met een hoog privacyrisico wordt eerst een Data Protection Impact Assessment (DPIA) uitgevoerd. Een DPIA brengt in kaart hoe groot de kans is dat de privacy van betrokkenen wordt geschaad, waar de risico's liggen en welke gevolgen dit kan hebben. Op basis van de uitkomsten van de DPIA neemt Invitare maatregelen om deze risico's te verkleinen.

6.8 Uitwisseling persoonsgegevens

Een verwerker is een partij die in opdracht van Invitare persoonsgegevens verwerkt, zoals een leverancier van een leerling administratiesysteem. Als Invitare een verwerker inschakelt om persoonsgegevens te verwerken, dan worden privacyafspraken vastgelegd in een verwerkersovereenkomst.
Bepaalt Invitare samen met één of meerdere partijen het doel en middelen voor de verwerking van persoonsgegevens? Dan is sprake van een zogenaamde gezamenlijke verwerkingsverantwoordelijkheid. In dat geval worden ook contractuele afspraken gemaakt rondom de zorgvuldige en veilige verwerking van gegevens.

Persoonsgegevens kunnen ook beschikbaar worden gesteld aan partijen die niet als verwerkers worden aangemerkt, maar als 'derden'. Deze derden verwerken persoonsgegevens niet in opdracht van een verwerkingsverantwoordelijke, maar voor hun eigen doel. Een verwerkersovereenkomst is daarom ook niet nodig, maar er moet wel een grondslag bestaan om de persoonsgegevens te delen. Denk aan de situatie waarin Invitare gegevens over medewerkers deelt met de Belastingdienst ten behoeve van de loonaangifte. De Belastingdienst verwerkt deze gegevens voor haar eigen wettelijke doeleinden en handelt niet als verwerker.

Gegevensverwerking buiten de EER

Schakelt Invitare een verwerker in uit een land buiten de Europese Economische Ruimte (EER) dat geen passend beschermingsniveau biedt? Dan gelden aanvullende voorwaarden.

- Bij een gegevensdeling buiten de EER moeten namelijk (juridische, technische en organisatorische) waarborgen zijn genomen om het beschermingsniveau ook buiten de EER te laten voldoen aan de AVG, zodat de persoonsgegevens voldoende beschermd blijven. Om dit te bereiken is meer nodig dan alleen het sluiten van een verwerkersovereenkomst. In dat geval maakt Invitare gebruik van de Europese modelcontracten, de zogenaamde 'Standard Contractual Clauses', en neemt Invitare aanvullende risico gebaseerde beveiligingsmaatregelen. Ook vindt voorafgaand aan de gegevensdeling afstemming plaats met de privacy officer en afdeling informatiebeveiliging om te beoordelen of de getroffen maatregelen voldoende zijn.

NB: De bepalingen van de meest recente versie van het convenant 'Digitale onderwijsmiddelen en privacy' zijn leidend bij het maken van afspraken met leveranciers, die als verwerkers in opdracht van de school persoonsgegevens verwerken.

6.9 Rechten van betrokkenen

Betrokkenen hebben op grond van de AVG recht op controle op de verwerking van hun persoonsgegevens. Een betrokkene kan onder andere gebruikmaken van het recht op inzage, rectificatie, verwijdering en bezwaar.
Leerlingen, leraren en andere medewerkers kunnen een verzoek tot uitoefening van deze rechten indienen via: privacy@stichting-invitare.nl .

Ook hebben betrokkenen het recht een klacht in te dienen bij de Autoriteit Persoonsgegevens. Invitare draagt er zorg voor dat de informatie over het uitoefenen van deze rechten op een transparante manier is verstrekt aan betrokkenen via een privacyverklaring.
Invitare zal binnen de wettelijke termijnen, uiterlijk binnen één maand, schriftelijk reageren op het verzoek. In uitzonderlijke situaties kan de reactietermijn worden verlengd, maar dan wordt dit wel binnen een maand gecommuniceerd. Voor AVG-verzoeken geldt een identificatieplicht, zodat de identiteit van de verzoeker kan worden vastgesteld. Hiertoe kan Invitare om extra informatie verzoeken, maar zal hierbij terughoudend zijn met het verzoeken om een kopie identiteitsbewijs.

7 Verantwoording IBP

7.1 Naleving AVG

Er vindt toezicht plaats door Invitare op de naleving van de normen uit dit beleid. Van belang is dat bestuurder, directeuren, privacy officers en de functionaris gegevensbecherming hun verantwoordelijkheid nemen en medewerkers aanspreken in geval van tekortkomingen. Invitare besteedt in dit verband actief aandacht aan informatiebeveiliging en privacy bij de aanstelling van medewerkers, tijdens functioneringsgesprekken en via bewustwordingscampagnes.

Mocht de naleving van dit beleid ernstig tekortschieten, dan kan Invitare de betrokken verantwoordelijke medewerkers maatregelen opleggen binnen de kaders van de CAO en toepasselijke wetgeving. Voor toezicht op de naleving van de AVG vervult de functionaris gegevensbescherming (FG) een belangrijke rol. De FG kan bijvoorbeeld informatie verzamelen over gegevensverwerkingen en beoordelen of deze aan de AVG voldoen. Ook kan de FG adviezen en aanbevelingen verschaffen aan Invitare.

7.2 Rapportage

Invitare heeft de verantwoordelijkheid om het IBP-beleid formeel goed te keuren en te monitoren of het IBP-beleid door de organisatie wordt toegepast. Periodiek (jaarlijks) wordt hierover gerapporteerd in de jaarverslaglegging van Invitare.
In dit beleidsdocument staan diverse actiepunten. Deze actiepunten komen voort uit de 0-meting van januari 2025. Vanuit de werkgroep wordt een planning van gewenste activiteiten gemaakt tot augustus 2027. De leden van de werkgroep, in passende samenstelling, zijn verantwoordelijk voor de realisatie hiervan. Waar mogelijke zoeken we hierin de samenwerking.

7.3 Beleidsherziening

Het IBP-beleid wordt door Invitare tenminste vierjaarlijks geëvalueerd en indien nodig herzien. Bij een substantiële wijziging van het IBP-beleid of in geval van belangrijke ontwikkelingen of veranderingen in wet- en regelgeving, volgt indien nodig een beleidswijziging.