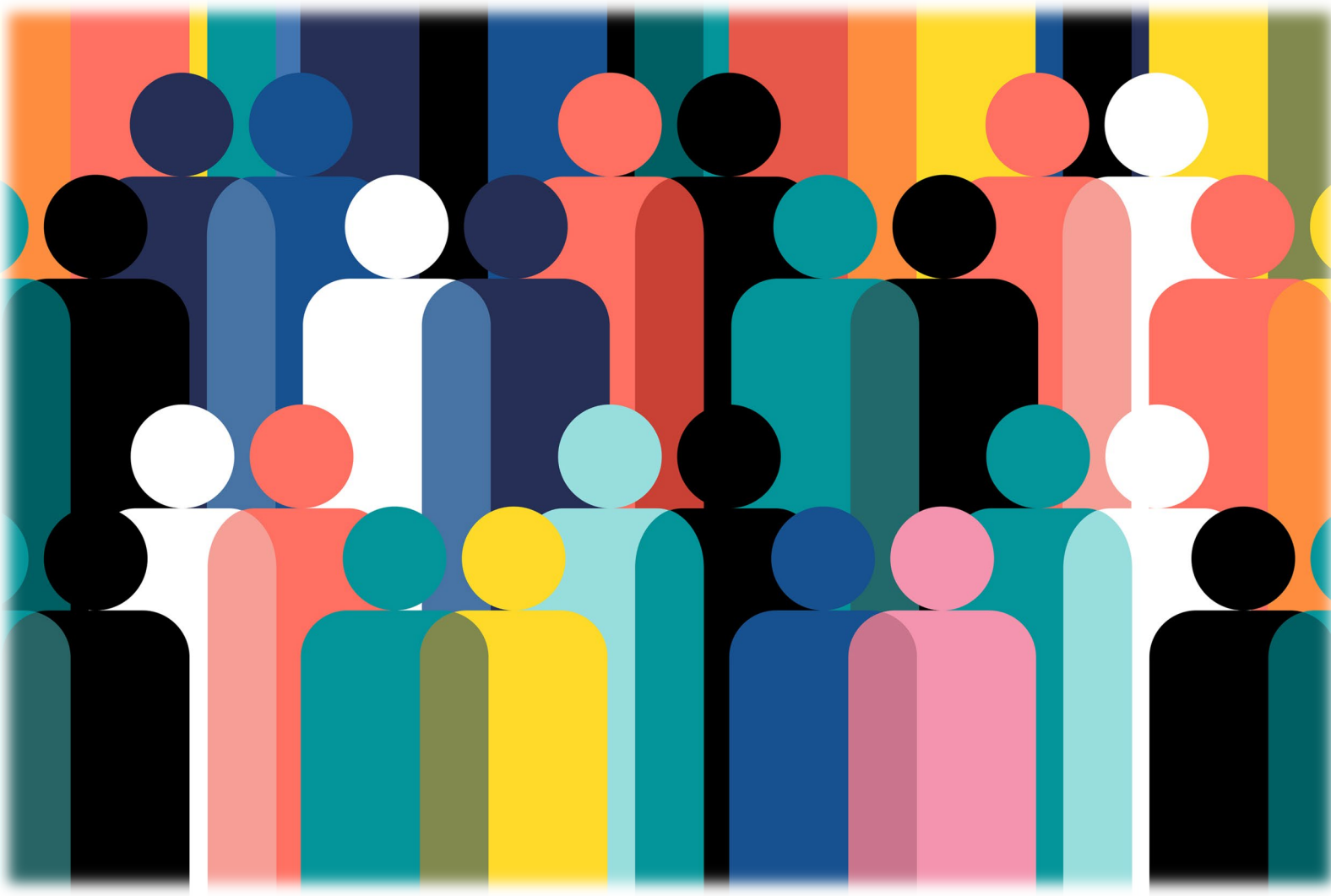
Samen aanjagen van vernieuwing

SURF Toetsingskader Privacy



Inhoudsopgave

Colofon

Ontwikkeling en beheer bij SURF

Het Toetsingskader Privacy is tot stand gekomen in samenwerking met vertegenwoordigers van diverse instellingen, organisaties en samenwerkingsverbanden uit de onderwijssector. Met dank aan in het bijzonder:

Anita Polderdijk	Hogeschool Windesheim
Barbara Gerretsen	Universiteit van Amsterdam
Erik van den Beld	Audittrail / SURF
Gisa de Jonge	Fontys Hogeschool
Jan van den Berg	Hogeschool van Amsterdam
Job Vos	SIVON
Kees-jan van Klaveren	Hogeschool Rotterdam
Loes van Zuijdam	Kennisnet
Marion van der Zwaan	Hogeschool van Amsterdam
Max de Bruin	Tilburg University
Niels Dutij	MBO Digitaal
Peter Vermeijs	MBO Raad
Raoul Winkens	Universiteit van Maastricht
Ronald Sarelse	Radboud Universiteit
Vera Heusschen	Hogeschool Leiden

Vanuit SURF werkten mee René Ritzen en Abdul Altawekji.

Naam document

SURFaudit Toetsingskader Privacy

Versienummer en -datum

Versie 3.1, 18 november 2024

Beheer

Het beheer van dit document berust vanaf mei 2025 bij het Privacy Expertise Centrum van SURF. Voor vragen over dit toetsingskader, neem contact op via e-mailadres: pec@surf.nl.

Rechten en vrijwaring

SURF is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. SURF aanvaardt geen enkele aansprakelijkheid voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. SURF aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Bron

Inleiding

Het Toetsingskader Privacy Onderwijs kent zeven domeinen die aansluiten bij de hoofdstukken uit de Algemene verordening gegevensbescherming (AVG). De domeinen zijn zo gekozen dat ze zo goed mogelijk aansluiten bij de praktijk in de onderwijssector. De domeinen zijn:

1. Beleid
2. Processen
3. Organisatorische inbedding
4. Rechten van betrokkenen
5. Samenwerking
6. Beveiliging
7. Verantwoording

Elk domein beschrijft een risico met bijbehorende beheerdoelstelling en vijf volwassenheidsniveaus. Voor iedere beheerdoelstelling zijn maatregelen beschreven die je helpen om op het gewenste volwassenheidsniveau uit te komen en te blijven (via een doorlopende verbetercyclus). De combinatie van risico, beheerdoelstelling, en volwassenheidsniveaus noemen we een statement. Dit toetsingskader bevat 25 statements (25 rijen) verdeeld over de zeven domeinen. Aan de hand van de volwassenheidsniveaus kan de organisatie bepalen wat het ambitieniveaus is en een GAP-analyse uitvoeren.

Voor elk volwassenheidsniveau is specifiek aangegeven welke maatregelen minimaal ingevoerd moeten zijn om het betreffende niveau te bereiken. Om aan een bepaald volwassenheidsniveau te voldoen, moeten je de vermelde maatregelen van dat niveau én de maatregelen van de onderliggende niveaus naleven. Niveaus 1 en 2 zijn hierbij minder relevant omdat er meestal geen of minimale maatregelen zijn genomen en is de uitvoering niet consequent. Niveau 2 is vooral een tussenstap tussen niveau 1 en 3 op basis waarvan je inzichtelijk krijgt welke groeistappen mogelijk zijn. De groei kan zo geleidelijk plaatsvinden. *Voorbeeld: om niveau 5 te kunnen behalen, moeten aan alle maatregelen van de niveaus 3, 4 en 5 zijn voldaan.*

Daar waar we in dit document spreken over bescherming van persoonsgegevens, wordt soms ook het woord ‘privacy’ gebruikt zodat de tekst beter leesbaar is. Denk bijvoorbeeld aan de woorden privacybeleid, privacyverklaring en privacymaatregelen. Dit komt ook de herkenbaarheid ten goede.

De beheerdoelstellingen in het domein beveiliging
Artikel 32 van de AVG zegt onder andere dat de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen. Daar waar dit over informatiebeveiliging gaat, is het van belang om de relevante statements uit het toetsingskader voor informatiebeveiliging te gebruiken, zodat je geen dingen dubbel doet, zie GB.03. Bij de jaarlijkse benchmark (zie hieronder) neem je die scores ook over mits die scores niet ouder zijn dan een jaar.

Jaarlijkse benchmark via SURFaudit

Dit toetsingskader vormt de basis voor de volwassenheidsmeting binnen de onderwijssector. Met het kader kun je als instelling je mate van volwassenheid in het beschermen van persoonsgegevens beoordelen. Het kan ook dienen als uitgangspunt voor uiteenlopende verbeterinitiatieven binnen de sector en als gids fungeren. De meting legt voornamelijk de focus op de volwassenheid van de processen omtrent de bescherming van persoonsgegevens en de mate waarin bescherming van persoonsgegevens processen zijn geïntegreerd in de overkoepelende bedrijfsprocessen. Het doel is niet om te bepalen of de organisatie AVG-compliant is.

Domein Beleid

BL.01 - Privacybeleid

Wat	Beschrijving
Domein	Beleid
Categorie	Privacybeleid
Beschrijving risico	Zonder privacybeleid heeft de organisatie geen duidelijke richtlijnen over hoe zij uitvoering geeft aan de verplichtingen die op haar rusten m.b.t. de bescherming van persoonsgegevens. Hierdoor worden persoonsgegevens mogelijk onrechtmatig verwerkt en kan de organisatie niet kan aantonen dat zij persoonsgegevens verwerkt in overeenstemming met AVG en UAVG. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen. Voor de organisatie: • imago- of reputatieschade • gebrek aan vertrouwen • dwangmaatregelen of boetes opgelegd door de toezichthouder
Beheerdoelstelling	Er is privacybeleid vastgesteld voor de gehele organisatie.
Toelichting	De organisatie dient aantoonbaar uitvoering te geven aan de privacybeginselen op grond van art. 5 lid 2 AVG (verantwoordingsplicht). Met formeel vastgesteld verstaan we dat het College van Bestuur (of Raad van Bestuur) het privacybeleid heeft vastgesteld. Het beleid is leidend voor de gehele organisatie en is een betrouwbare bron van informatie met betrekking tot bescherming van persoonsgegevens. Dit draagt bij aan een consistente en uniforme naleving van de AVG en voorkomt verwarring of tegenstrijdigheden binnen de organisatie. Binnen sommige domeinen, bijvoorbeeld onderwijs en onderzoek, is sectorspecifieke wetgeving van toepassing, zoals onderzoek naar mensen, of wetgeving over minderjarige onderwijsdeelnemers. De organisatie kan ervoor kiezen om hiervoor domeinspecifiek beleid vast te stellen. In dit specifieke beleid worden het privacybeleid en het beleid dat volgt uit de sectorspecifieke wet- en regelgeving opgenomen.
Toetsing	O&P
VWN1 - ad hoc	a. Het privacybeleid bestaat in concept of er is geen beleid opgesteld.
VWN2 - herhaalbaar	a. Privacybeleid en uitwerkingen daarvan bestaan, maar ze zijn onvolledig, verouderd, (nog) niet formeel vastgesteld en/of alleen bekend bij enkele individuen in de organisatie.
VWN3 - bepaald	a. Het privacybeleid is actueel en beschrijft hoe de organisatie uitvoering geeft aan de privacybeginselen die in art 5 lid 1 AVG zijn vastgelegd. b. Het privacybeleid beschrijft de verplichtingen zoals rechtmatigheid, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid die op de organisatie rusten op grond van relevante privacywetgeving en beschrijft hoe de organisatie uitvoering geeft aan deze verplichtingen. c. Het privacybeleid is formeel door het hoogste management vastgesteld en organisatiebreed bekend, makkelijk vindbaar en makkelijk te begrijpen. d. In het beleid is rekening gehouden met (sector-) specifieke wet- en regelgeving, indien van toepassing. e. Wijzigingen in het beleid worden gecommuniceerd.
VWN4 - beheerst	a. Het privacybeleid wordt periodiek, maar ten minste eenmaal per 36 maanden, geëvalueerd en zo nodig herzien.

Wat	Beschrijving
	b. De actualiteit en kwaliteit van het privacybeleid worden getoetst in samenhang met overige beleidsstukken en vice versa. Veranderde wet- en regelgeving en doelstellingen van de organisatie vormen hier een onderdeel van.
VWN5 - geoptimaliseerd	a. Er wordt in het privacybeleid rekening gehouden met toekomstige veranderende wet- en regelgeving, doelstellingen en visie van de organisatie. b. Er wordt actief verbinding gezocht met andere (vergelijkbare) organisaties om kennis, ervaring en best practices uit te wisselen.
AVG-UAVG	AVG 24 lid 2
ISO 27701:2019	6.2
VNG 3.0	1.2
Norea PCF	• PP001 • PP002 • PP003 • PP004 • DMI02 • ULI02 • RRE054 • RRE055

BL.02 - Rollen, taken en verantwoordelijkheden

Wat	Beschrijving
Domein	Beleid
Categorie	Rollen, taken en verantwoordelijkheden
Beschrijving risico	Het ontbreken van duidelijke rollen, taken en verantwoordelijkheden kunnen ertoe leiden dat noodzakelijke taken gerelateerd aan de bescherming van persoonsgegevens niet of niet correct worden uitgevoerd. Dit kan tot gevolg hebben dat de organisatie niet adequaat reageert op privacy gerelateerde incidenten, vragen of klachten en potentiële privacyschendingen onopgemerkt blijven. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen. Voor de organisatie: • imago- of reputatieschade • dwangmaatregelen of boetes opgelegd door de toezichthouder • schadeclaims van gedupeerden.
Beheerdoelstelling	Rollen, taken en verantwoordelijkheden met betrekking tot privacy binnen de lijnorganisatie zijn benoemd, belegd en vastgelegd in het privacybeleid.
Toelichting	Aanbevolen wordt om een RASCI matrix te hanteren en dit in het privacybeleid vast te leggen. Voor een uitleg van RASCI, zie: • Privacy Governance, platform IV-HO Een leidraad hierbij kan ook zijn 3-lines model zijn.
Toetsing	O&P
VWN1 - ad hoc	a. Rollen, taken en verantwoordelijkheden met betrekking tot privacy zijn niet duidelijk gedefinieerd en toegewezen binnen de organisatie of zijn niet gedocumenteerd.
VWN2 - herhaalbaar	a. Rollen, taken en verantwoordelijkheden zijn binnen de organisatie deels of informeel belegd en/of zijn sterk afhankelijk van de ondersteunende (centrale) privacyorganisatie of privacy officers.
VWN3 - bepaald	a. Rollen, taken en verantwoordelijkheden met betrekking tot privacy zijn formeel benoemd, belegd en vastgelegd in het privacybeleid en organisatiebreed bekend. b. Vastgelegd is dat het hoogste management eindverantwoordelijk is voor privacy binnen de organisatie en dat lijnmanagers verantwoordelijk zijn voor privacy binnen hun managementdomein. c. Binnen de organisatie is vastgesteld welke functionaris bevoegd is om keuzes te maken op het gebied van privacyrisico's, het treffen van mitigerende maatregelen en het accepteren van restrisico's.
VWN4 - beheerst	a. Het lijnmanagement legt aantoonbaar verantwoording af over haar taken en verantwoordelijkheden met betrekking tot privacy. b. De organisatie evalueert periodiek of de rollen taken en verantwoordelijkheden met betrekking tot privacy nog passend en effectief zijn, en voert indien nodig verbeteringen door.
VWN5 - geoptimaliseerd	a. De organisatie monitort proactief of rollen, taken en verantwoordelijkheden met betrekking tot privacy nog passend en actueel zijn, in lijn met ontwikkelingen én met wet- en regelgeving. b. Rollen, taken en verantwoordelijkheden met betrekking tot privacy zijn expliciet opgenomen in de functieprofielen van de organisatie, waarmee ze een integraal onderdeel zijn van de taken en verantwoordelijkheden van elke medewerker.

Wat	Beschrijving
	c. De organisatie hanteert een 'lessons learnt'-benadering om haar privacyverantwoordelijkheden continu te verbeteren, op basis van ervaringen uit het verleden en verwachtingen voor de toekomst.
AVG-UAVG	AVG 24 lid 2 38
ISO 27701:2019	6.3
VNG 3.0	1.3
Norea PCF	• PP002 • RRE05 • RMA04

BL.03 – Risico's

Wat	Beschrijving
Domein	Beleid
Categorie	Risico's
Beschrijving risico	Een gebrek aan inzicht in risico's bij de verwerking van persoonsgegevens kan ertoe leiden dat er geen of onvoldoende passende maatregelen (organisatorisch en technisch) worden genomen om de risico's te beperken. Dit kan leiden tot onrechtmatige verwerking en/of onvoldoende beveiliging van persoonsgegevens. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen. Voor de organisatie: • imago- of reputatieschade • dwangmaatregelen of boetes opgelegd door de toezichthouder • schadeclaims van gedupeerden. • hogere kosten door naderhand (reparatie-) maatregelen te moeten nemen. • mogelijk slechte datakwaliteit.
Beheerdoelstelling	De organisatie heeft (organisatiebreed) inzicht in de risico's van de verwerking van persoonsgegevens en behandelt deze op een adequate wijze.
Toelichting	Deze statement gaat niet over het uitvoeren van DPIA's voor verwerkingen die een hoog risico voor betrokkenen kunnen opleveren, maar om het consistent en periodiek kunnen identificeren, beoordelen en beheren van (organisatiebreed) risico's met als doel breed inzicht in risico's bij de verwerking van persoonsgegevens te verkrijgen. Dit statement richt zich op het consistent en periodiek kunnen identificeren, beoordelen en beheren van (organisatiebreed) risico's met als doel breed inzicht in risico's bij de verwerking van persoonsgegevens te verkrijgen. Dit omvat het hebben van een formeel proces voor risico-identificatie, -beoordeling en -beheer, evenals de documentatie van hoge risico's en toegewezen verantwoordelijken. Het proces zorgt ervoor dat risicoacceptatie op het juiste (verantwoordelijke) managementniveau plaatsvindt en omvat een beoordelingskader voor risicomitigatie. Bovendien is er een continue evaluatie en verbetering van de risicobeheersingsmaatregelen.
Toetsing	O&P
VWN1 - ad hoc	a. Er is geen gedocumenteerd proces binnen de organisatie voor het identificeren, beoordelen en beheren van risico's in de verwerking van persoonsgegevens. b. De organisatie heeft beperkt inzicht in de risico's bij de verwerking van persoonsgegevens.
VWN2 - herhaalbaar	a. De organisatie heeft een informeel proces geïmplementeerd voor het identificeren, beoordelen en beheren van hoge risico's in de verwerking van persoonsgegevens.
VWN3 - bepaald	a. De organisatie heeft een informeel proces geïmplementeerd voor het identificeren, beoordelen en beheren van hoge risico's in de verwerking van persoonsgegevens.
VWN4 - beheerst	a. Er is een volledige registratie van alle risico's, ook de lage geïdentificeerde risico's. b. Alle geïdentificeerde risico's worden volledig geregistreerd en systematisch beheerd. c. De doeltreffendheid van het proces voor het identificeren, beoordelen en beheren van risico's én de risicobeheersmaatregelen worden periodiek beoordeeld en, zo nodig, aangepast.
VWN5 - geoptimaliseerd	a. De organisatie heeft een proactieve en geïntegreerde benadering van risicobeheer, waarbij de risico's in de verwerking van persoonsgegevens continu worden gemonitord

Wat	Beschrijving
	en aangepast in reactie op veranderingen in zowel de interne organisatie als het externe landschap. b. Het management controleert en evalueert continu de doeltreffendheid van haar risicobeheersysteem en voert waar nodig verbeteringen door.
AVG-UAVG	AVG 32 AVG 24 lid 1
ISO 27701:2019	5.4
VNG 3.0	6.1
Norea PCF	• RMA01 • RMA03 • RMA04 • RMA05 • BD02 • ISP01 • ISP03 • MON01 • MON02 • MON03 • REV01

Processen

PR.01 - Operationele processen

Wat	Beschrijving
Domein	Processen
Categorie	Operationele processen
Beschrijving risico	Wanneer de organisatie geen duidelijk beeld heeft van de operationele processen waarin persoonsgegevens worden verwerkt en/of deze processen niet heeft beschreven of deze beschrijvingen niet actueel zijn, kan dit leiden tot ongecontroleerde en mogelijk onrechtmatige verwerkingen. Door het ontbreken van een duidelijk overzicht en inzicht in de operationele processen kan de organisatie niet of niet voldoende aantonen dat de verwerkingen van persoonsgegevens in overeenstemming met de AVG worden uitgevoerd (art. 24 lid 1 AVG). Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen indien persoonsgegevens onbedoeld worden gedeeld, ingezien, gewijzigd of worden verloren. Voor de organisatie: • slechte datakwaliteit en hogere kosten door het nemen van verkeerde beslissingen bij de verwerking van persoonsgegevens.
Beheerdoelstelling	De organisatie heeft de operationele processen waarin persoonsgegevens worden verwerkt in beeld en beschreven.
Toelichting	Deze maatregel heeft betrekking op de operationele (uitvoerende) processen binnen de onderwijssector die van invloed kunnen zijn voor onderwijsdeelnemers, onderzoekparticipanten, of de organisatie zelf. Het inzichtelijk hebben van operationele processen en de IT systemen die daar ondersteunend aan zijn vormt een belangrijk aanknopingspunt om gegevensverwerkingen te identificeren en te beheersen. Zowel processen die noodzakelijk zijn voor de dienstverlening van de organisatie als ondersteunende processen (bijvoorbeeld HR-processen) behoren inzichtelijk te zijn. Omdat de AVG van een risicogebaseerde aanpak uitgaat, kan de focus in eerste instantie gericht zijn op processen die een hoog risico vormen voor betrokkenen.
Toetsing	O&P
VWN1 - ad hoc	a. De organisatie heeft geen systematische en gestructureerde aanpak voor het identificeren en documenteren van operationele processen waarin persoonsgegevens worden verwerkt. b. Er is beperkt of geen inzicht in de processen waarin persoonsgegevens worden verwerkt, met name in de processen met een hoog risico voor de betrokkenen.
VWN2 - herhaalbaar	a. De organisatie heeft een gedeeltelijk systematische en gestructureerde aanpak voor het identificeren en documenteren van operationele processen waarin persoonsgegevens worden verwerkt. Deze aanpak wordt niet consistent en/of organisatiebreed gehanteerd. b. Voor enkele processen waarin persoonsgegevens worden verwerkt is een procesbeschrijving met daarin minimaal een titel van het proces en een verantwoordelijke proceseigenaar, maar er is geen centraal overzicht of register van deze processen.
VWN3 - bepaald	a. De organisatie hanteert organisatiebreed een systematische en gestructureerde aanpak voor het identificeren en documenteren van processen waarin persoonsgegevens worden verwerkt en heeft inzicht in de processen waarin persoonsgegevens worden verwerkt. Ten minste de processen met een hoog risico voor betrokkenen zijn beschreven en vastgelegd. b. Proceseigenaren zijn aangewezen en zijn verantwoordelijk voor de periodieke evaluatie van de procesbeschrijving en passen deze zo nodig aan.
VWN4 - beheerst	a. De organisatie heeft alle operationele processen waarin persoonsgegevens worden verwerkt vastgelegd en beschreven (niet alleen die met hoog risico).

Wat	Beschrijving
	b. De organisatie voert periodieke evaluaties uit van de processen, waarin persoonsgegevens worden verwerkt, om de bescherming van persoonsgegevens te waarborgen en voert waar nodig verbeteringen door. c. Binnen een vastgesteld interval wordt geëvalueerd of de beschrijving van het proces aansluit bij de praktijk. d. Proceseigenaren informeren proactief over de realisatie van uitgevoerde wijzigingen naar aanleiding van evaluaties
VWN5 - geoptimaliseerd	a. Het management ziet het belang in van procesmatig werken en het actueel houden van operationele processen en stuurt hier actief op. b. Het management (eventueel in samenspraak met proceseigenaren) houdt toekomstige ontwikkelingen in beeld en laat deze proactief meenemen in de (her-)definitie van processen en aanwijzing van proceseigenaren. c. Er wordt pro-actief geborgd dat wijzigingen en initiatieven die niet voldoen aan het privacybeleid worden geïdentificeerd en opgelost.
AVG-UAVG	AVG 24 lid 1
ISO 27701:2019	-
VNG 3.0	2.1
Norea PCF	• PDI01

PR.02 - Verwerkingsregister inrichten

Wat	Beschrijving
Domein	Processen
Categorie	Verwerkingsregister inrichten (opzet en vastlegging verwerkingen)
Beschrijving risico	Het ontbreken van een volledig en actueel verwerkingsregister kan ertoe leiden dat de organisatie onvoldoende inzicht heeft in de verwerking van persoonsgegevens. Hierdoor kan de organisatie niet voldoende aantonen dat ze aan de privacywetgeving voldoet. Dit kan leiden tot: Voor betrokkenen: • onrechtmatige verwerkingen. • onjuiste informatieverstrekking over de verwerking van hun gegevens. • vertraging bij de uitvoering van hun rechten. • risico's voor hun rechten en vrijheden, zoals wijzigingen in het gebruiksdoel, ongedocumenteerde verstrekking aan derden, of doorgifte naar derde landen. Voor de organisatie: • imago- of reputatieschade. • dwangmaatregelen, boetes door de toezichthouder of schadeclaims van gedupeerden. • hogere kosten door het nemen van (reparatie-) maatregelen achteraf. • onvolledige meldingen of vertraging in relatie tot de meldplicht datalekken. • mogelijk slechte datakwaliteit.
Beheerdoelstelling	De organisatie houdt een verwerkingsregister bij wettelijke eisen.
Toelichting	We adviseren om de verwerkingen op domein- (Onderwijs, Onderzoek en Bedrijfsvoering) / afdelings- / proces-niveau inzichtelijk te maken. Naast de wettelijk voorgeschreven velden (art. 30 lid 1 en lid 2 AVG) wordt geadviseerd om het verwerkingsregister ook te gebruiken als tool om additionele registraties bij te houden. Bijvoorbeeld of een DPIA moet worden uitgevoerd en indien dit het geval is wanneer deze is uitgevoerd. Het register is opgesteld in een vorm die het mogelijk maakt om het gemakkelijk te delen met de autoriteiten. De AP heeft het recht om inzicht in het register te vorderen, bijvoorbeeld in geval van mogelijke schendingen van de AVG of onderzoeken naar de naleving ervan. (art. 30 lid 4 AVG). In de rol van verwerkingsverantwoordelijke dient het verwerkingsregister per verwerking ten minste de volgende informatie te bevatten: • naam en contactgegevens van de verwerkingsverantwoordelijke, en van de functionaris gegevensbescherming. De verwerkingsverantwoordelijke kan bijvoorbeeld degene zijn die binnen de organisatie verantwoordelijk voor de gegevens is, meestal de proceseigenaar. • de AVG-rol (verwerkingsverantwoordelijke, verwerker, gezamenlijk verantwoordelijke). • verwerkingsdoeleinden (bijvoorbeeld registratie onderwijsdeelnemers). • de grondslag voor verwerking. • categorieën betrokkenen (bijvoorbeeld onderwijsdeelnemers websitebezoekers en medewerkers). • categorieën persoonsgegevens (bijvoorbeeld NAW-gegevens, contactgegevens, financiële gegevens). • categorieën ontvangers (bijvoorbeeld ICT-dienstverleners). • informatie over eventuele doorgifte van persoonsgegevens naar een derde land. • of er sprake is van doorgifte van persoonsgegevens naar land buiten de EER, en zo ja, welk land dit is. • bewaartermijnen voor de verschillende categorieën van persoonsgegevens. • beveiligingsmaatregelen.
Toetsing	O
VWN1 - ad hoc	a. Er is geen verwerkingsregister of er zijn geen verwerkingen bijgehouden.

Wat	Beschrijving
	b. Wettelijk vereiste onderdelen, rollen voor verwerking (verwerkingsverantwoordelijke, verwerker, gezamenlijke verwerkingsverantwoordelijken) en verwijzingen naar operationele processen zijn niet duidelijk of ontbreken.
VWN2 - herhaalbaar	a. Er is een (gedeeltelijk) ingevuld verwerkingsregister, maar niet alle wettelijk vereiste onderdelen zijn aanwezig. b. Voor (sommige) verwerkingen zijn de rollen voor verwerking niet duidelijk of niet gedocumenteerd. c. Een deel van de verwerkingen is getoetst aan de privacybeginselen zoals beschreven in art. 5 lid 1 AVG
VWN3 - bepaald	a. Het verwerkingsregister bevat minimaal alle wettelijk vereiste onderdelen (art. 30 lid 1 AVG voor de verwerkingsverantwoordelijk of voor de verwerker lid 2). b. Voor elke vastgelegde verwerking is duidelijk wie de verwerkingsverantwoordelijke, de verwerker of de gezamenlijke verwerkingsverantwoordelijken zijn. c. De verwerkingen met persoonsgegevens zijn vastgelegd en zijn getoetst aan de privacy beginselen uit art. 5 lid 1 AVG.
VWN4 - beheerst	a. Indien de AP inzicht in het verwerkingsregister vraagt, kan dit op eenvoudige wijze worden voorgelegd.
VWN5 - geoptimaliseerd	a. Het verwerkingsregister wordt actief gebruikt voor risicobeheer en besluitvorming. Het is niet alleen een database voor naleving, maar een belangrijk instrument voor de privacycultuur binnen de organisatie. b. In het verwerkingsregister staan verwijzingen naar DPIA, verwerkersovereenkomst en andere relevante overeenkomsten. c. Het register bevat volledige en actuele verwijzingen naar alle operationele processen waarbinnen persoonsgegevens worden verwerkt.
AVG-UAVG	AVG 30
ISO 27701:2019	7.2.8
VNG 3.0	2.2
Norea PCF	• PIA???? • PDI02 • PDI03 • PDI04 • DTR01 • PPO05 • PDI03 • LRC01 • CFR03 • DMI01 • URE03 • ACD01 • ACD02 • RRE05

PR.03 - Verwerkingsregister actualiseren

Wat	Beschrijving
Domein	Processen
Categorie	Verwerkingsregister actualiseren
Beschrijving risico	Het onnauwkeurig of inconsistent bijwerken van het verwerkingsregister kan ertoe leiden dat de organisatie niet volledig conform de AVG handelt. Daardoor kan de organisatie een onjuist beeld krijgen van de werkelijke omvang en aard van de verwerking van persoonsgegevens. Hierdoor kunnen incidenten over het hoofd worden gezien vanwege onduidelijkheid over de verwerking van deze gegevens. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen bijvoorbeeld door wijziging in gebruiksdoel, niet (volledig) gedocumenteerde verstrekking aan derden, (gewijzigde) doorgifte naar derde landen. • onrechtmatige verwerkingen. • onjuiste informatieverstrekking aan onderwijsdeelnemers, onderzoeksdeelnemers en medewerkers. • vertraging of onmogelijkheid bij de uitvoering van hun rechten. • risico's zoals wijzigingen in gebruiksdoel, ongedocumenteerde gegevensverstrekking of doorgifte naar derde landen. Voor de organisatie: • imago- of reputatieschade. • dwangmaatregelen, boetes door de toezichthouder of schadeclaims van gedupeerden • vertragingen of fouten in meldingen in verband met de meldplicht datalekken. • hogere kosten door naderhand (reparatie-) maatregelen te moeten nemen. • verminderde datakwaliteit.
Beheerdoelstelling	De organisatie houdt het verwerkingsregister continu actueel.
Toelichting	In het verwerkingsregister is het zichtbaar / aantoonbaar dat beheer en bijstelling (regelmatig) plaatsvindt, b.v. door wijzigingsdata te vermelden.
Toetsing	P
VWN1 - ad hoc	a. Er is geen duidelijke procedure voor het bijhouden van nieuwe en gewijzigde verwerkingen in het verwerkingsregister.
VWN2 - herhaalbaar	a. Er is een informele procedure voor het bijhouden van nieuwe en gewijzigde verwerkingen in het verwerkingsregister, maar deze wordt niet consequent toegepast. b. Het verwerkingsregister is niet up-to-date omdat wijzigingen in verwerkingen niet altijd tijdig in het verwerkingsregister worden opgenomen c. De verantwoordelijkheden voor het bijhouden van het verwerkingsregister zijn toegewezen, maar worden niet actief opgepakt.
VWN3 - bepaald	a. Er is een vastgestelde procedure die definieert hoe en wanneer nieuwe en gewijzigde verwerkingen in het verwerkingsregister worden opgenomen. b. Bij wijzigingen wordt opnieuw getoetst of de verwerking in overeenstemming is met de privacybeginselen uit art. 5 lid 1 AVG. c. Er is vastgesteld met welke frequentie het verwerkingsregister wordt beoordeeld op volledigheid en actualiteit, en welke functionaris verantwoordelijk is voor deze beoordeling. d. Wijzigingen en nieuwe initiatieven waarbij persoonsgegevens worden verwerkt, worden direct in het register opgenomen.
VWN4 - beheerst	a. Het actueel houden van het verwerkingsregister is, waar van toepassing, volledig geïntegreerd in de processen van de organisatie. Wijzigingen en nieuwe initiatieven waarbij persoonsgegevens worden verwerkt, worden direct in het register opgenomen.

Wat	Beschrijving
VWN5 - geoptimaliseerd	a. De organisatie heeft een tool ingezet voor het bijhouden en auditen van het verwerkingsregister.
AVG-UAVG	AVG 30
ISO 27701:2019	7.2.8
VNG 3.0	2.2
Norea PCF	• PDI04 • DTR01

PR.04 – Risicoinschatting (pre-DPIA)

Wat	Beschrijving
Domein	Processen
Categorie	Identificatie van risico's (met behulp van pre-DPIA's)
Beschrijving risico	Wanneer de organisatie niet systematisch risico's identificeert bij nieuwe of gewijzigde gegevensverwerkingen kan dit leiden tot onvoorziene gevolgen voor de privacy van betrokkenen, waaronder onderwijs- en onderzoeksdeelnemers. De introductie van nieuwe technologieën of producten. Denk hierbij ook aan nieuwe functionaliteit die regelmatig door cloudleveranciers wordt geïntroduceerzonder dat hiervoor een volledige beoordeling van de privacy-implicaties is uitgevoerd, kan leiden tot incidenten bij de verwerking van persoonsgegevens met ongewenste gevolgen voor de betrokkenen en de organisatie. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door onvoldoende of verkeerde maatregelen om de risico's te mitigeren. Voor de organisatie • imago- of reputatieschade. • dwangmaatregelen of boetes opgelegd door de toezichthouder. • schadeclaims van gedupeerden. • hogere kosten door naderhand (reparatie-) maatregelen te moeten nemen. • mogelijk slechte datakwaliteit.
Beheerdoelstelling	De organisatie identificeert systematisch of verwerkingen een hoog risico in kunnen houden voor de rechten en vrijheden van betrokkenen.
Toelichting	De criteria die bepalen of een verwerking een hoog risico vormt voor betrokkenen zijn opgenomen in de lijsten van de AP en EDPB: • AP, wanneer een DPIA? • Guideline DPIA EDPB Voor VWN3.a en VWN3.b geldt dat de methode met het in BL.03 beschreven risicobeoordelingsproces moet overeenkomen.
Toetsing	O&P
VWN1 - ad hoc	a. Er is geen procedure of methode (zoals een pre-DPIA) om te bepalen of nieuwe of gewijzigde gegevensverwerkingen een hoog risico kunnen vormen voor de privacy van betrokkenen. b. Er is geen systematische beoordeling van alle verwerkingen om te bepalen of deze een hoog risico kunnen opleveren.
VWN2 - herhaalbaar	a. Er is een informele procedure voor alle nieuwe en gewijzigde verwerkingen voor het identificeren van hoog risico verwerkingen, maar deze wordt niet consequent toegepast of is onvolledig. b. Niet alle verwerkingen zijn beoordeeld op een mogelijk hoog risico. c. De risicoanalyse die ten grondslag ligt aan de beslissing of een verwerking al dan niet een hoog risico kan opleveren, is niet gedocumenteerd en/of onvolledig.
VWN3 - bepaald	a. Er is een methode/procedure vastgesteld om voor alle nieuwe en gewijzigde verwerkingen te bepalen of deze mogelijkerwijs een hoog risico inhouden voor de rechten en vrijheden van betrokkenen. b. De methode/procedure om te bepalen of nieuwe en gewijzigde verwerkingen mogelijk een hoog risico vormen voor de rechten en vrijheden van betrokkenen, wordt consequent toegepast. c. Alle verwerkingen zijn beoordeeld op mogelijk hoog risico en deze zijn als zodanig aangemerkt in het verwerkingsregister.

Wat	Beschrijving
	d. De analyse die ten grondslag ligt aan de beslissing of een verwerking een hoog risico kan opleveren, is gedocumenteerd.
VWN4 - beheerst	a. Verwerkingen die waarschijnlijk een hoog risico inhouden, worden proactief geïdentificeerd en beheerd. b. De procedure voor het identificeren van hoog risico verwerkingen wordt periodiek geëvalueerd en zo nodig verbeterd. c. De analyse en documentatie van het besluit of een verwerking een hoog risico kan opleveren, is gemakkelijk te vinden en toegankelijk.
VWN5 - geoptimaliseerd	a. Het identificeren van hoog risico verwerkingen is volledig geïntegreerd in de operationele processen van de organisatie. b. Er is een cultuur van voortdurende risicobeoordeling waarbij alle verwerkingen consequent worden beoordeeld op een mogelijk hoog risico en dit wordt aantoonbaar vastgelegd (in het verwerkingsregister). c. De documentatie van de analyse en het besluit of een verwerking een hoog risico kan opleveren, is volledig, makkelijk vindbaar, transparant en wordt gezien als een krachtig hulpmiddel binnen de organisatie.
AVG-UAVG	AVG 35
ISO 27701:2019	7.2.5
VNG 3.0	2.3
Norea PCF	• PIA01 • RMA03 • PBD01 • LRC01

PR.05 - DPIA's

Wat	Beschrijving
Domein	Processen
Categorie	DPIA's
Beschrijving risico	Het niet uitvoeren van een DPIA voor verwerkingen die een hoog risico kunnen opleveren, of het niet adequaat opvolgen van de uitkomsten van DPIA's, kan leiden tot een onvolledig begrip van privacyrisico's. Dit kan ertoe leiden dat onvoldoende en/of verkeerde maatregelen worden genomen om deze risico's te mitigeren. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door onvoldoende of verkeerde maatregelen om de risico's te mitigeren. Voor de organisatie: • imago- of reputatieschade. • dwangmaatregelen of boetes opgelegd door de toezichthouder. • schadeclaims van gedupeerden. • hogere kosten door naderhand (reparatie-) maatregelen te moeten nemen. • mogelijk slechte datakwaliteit.
Beheerdoelstelling	Indien een verwerking is geïdentificeerd die een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen, wordt een DPIA uitgevoerd die aan de eisen van de AVG voldoet. De organisatie beheert de uitkomsten van DPIA's systematisch.
Toelichting	In beginsel is de verplichting om een DPIA uit te voeren beperkt tot verwerkingen waarvoor de organisatie verantwoordelijke is (dus ook indien er sprake is van gezamenlijke verwerkingsverantwoordelijkheid). Voor de uitvoering van een DPIA kan de organisatie zelf een model ontwikkelen of een reeds vastgesteld model toepassen. Wettelijke vereisten over DPIA's zijn o.a. hier te vinden: • AP uitvoeren DPIA We adviseren om de bevoegdheid voor afwijking van het advies van de FG toe te kennen aan een managementorgaan met passend mandaat. Dit zou doorgaans een functie zijn zoals een directeur, clustermanager, teammanager, of MT-lid.
Toetsing	O&P
VWN1 - ad hoc	a. Er is geen formele procedure vastgesteld voor het uitvoeren van DPIA's op nieuwe en sterk gewijzigde verwerkingen die mogelijk een hoog risico inhouden. b. De FG wordt (nog) niet betrokken of om advies gevraagd bij het uitvoeren van DPIA's.
VWN2 - herhaalbaar	a. Er is een procedure voor het uitvoeren van DPIA's, maar deze wordt niet altijd of niet organisatiebreed toegepast op nieuwe en gewijzigde verwerkingen die mogelijk een hoog risico inhouden. b. DPIA-rapporten worden wel opgesteld, maar voldoen niet altijd aan de wettelijke vereisten. c. Niet alle hoog-risico verwerkingen zijn onderworpen aan een DPIA. d. De FG wordt betrokken, maar het beslissingsproces over het afwijken van het advies van de FG is niet systematisch gedocumenteerd en is persoonsafhankelijk.
VWN3 - bepaald	a. Er is een vaste methode voor het uitvoeren van DPIA's, en die wordt toegepast op alle nieuwe en sterk gewijzigde verwerkingen die mogelijk een hoog risico inhouden. b. Er is een procedure vastgesteld voor het opvolgen (behandelen of accepteren) van risico's die in een DPIA zijn geïdentificeerd. c. DPIA-rapporten worden opgesteld volgens een gestandaardiseerd format dat voldoet aan de wettelijke vereisten. d. Alle hoog-risico verwerkingen zijn onderworpen aan een DPIA. e. Er is een standaardprocedure voor het documenteren van afwijkingen van het advies van de FG. Deze procedure wordt consequent gevolgd. f. De DPIA-rapportages zijn makkelijk vindbaar.

Wat	Beschrijving
VWN4 - beheerst	a. Het uitvoeren van DPIA's en het opvolgen (behandelen of accepteren) van risico's die in een DPIA zijn geïdentificeerd, maakt onderdeel uit van een (organisatiebreed) risicobeheerkader. b. DPIA's worden minstens elke 36 maanden opnieuw beoordeeld. c. Bij een afwijking van een FG-advies, legt het management onderbouwd vast waarom afgeweken is van het advies. d. In gevallen waar een geïdentificeerd risico niet gemitigeerd of geaccepteerd wordt, wordt dit expliciet gedocumenteerd en uitgelegd. e. Er is een overzicht van en inzicht in de uitgevoerde DPIA's, inclusief de data waarop deze zijn uitgevoerd of herzien. f. Periodiek wordt de effectiviteit van de DPIA-procedure geëvalueerd om continue verbetering te bevorderen.
VWN5 - geoptimaliseerd	a. Er is actieve betrokkenheid van het hoogste management bij het DPIA-proces, vooral wanneer er wordt afgeweken van het advies van de FG. b. De organisatie heeft periodiek overleg met andere organisaties en/of andere samenwerkingsverbanden om te leren van elkaars DPIA's en (de effectiviteit van) mitigerende maatregelen, met name bij soortgelijke verwerkingen. c. De organisatie heeft de effectiviteit en efficiëntie van haar DPIA-proces geoptimaliseerd, bijvoorbeeld door gebruik te maken van automatisering of geavanceerde tools. d. Bij de overdracht van een project, worden de DPIA en eventuele openstaande maatregelen in acht genomen. Ook wordt er actief naar risico's in de DPIA gevraagd door de betrokken projectmanagementteams.
AVG-UAVG	AVG 35 AVG 36
ISO 27701:2019	5.2.2 7.2.5
VNG 3.0	2.4
Norea PCF	• PIA01 • PIA02 • PIA04 • PIA05 • PIA06 • RMA05 • RRE04 • RRE05

PR.06 - Privacy by Design

Wat	Beschrijving
Domein	Processen
Categorie	Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by Design & Privacy by Default)
Beschrijving risico	Het niet consequent en tijdig toepassen van gegevensbescherming door ontwerp (Privacy by Design) en het niet hanteren van privacyvriendelijke standaardinstellingen (Privacy by Default) kunnen leiden tot onvoldoende bescherming van persoonsgegevens. Dit kan resulteren in onbedoelde verzameling, ongeoorloofd gebruik en ongeautoriseerde openbaarmaking van persoonsgegevens Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door onvoldoende of verkeerde Privacy by Design/Privacy by Default maatregelen. Voor de organisatie: • imago- of reputatieschade. • dwangmaatregelen of boetes opgelegd door de toezichthouder. • schadeclaims van gedupeerden. • hogere kosten door naderhand (reparatie-) maatregelen te moeten nemen. • mogelijk slechte datakwaliteit.
Beheerdoelstelling	Bij de ontwikkeling, het ontwerp, selectie en het gebruik van toepassingen, diensten en producten houdt de organisatie zo vroeg mogelijk rekening met de privacybeginselen en privacyrisico's, en past gegevensbescherming door ontwerp en standaardinstellingen toe. Toepassingen zijn standaard privacyvriendelijk ingesteld.
Toelichting	De privacybeginselen uit art. 5 lid 1 AVG zijn rechtmatigheid, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid. De organisatie dient aantoonbaar aan deze beginselen te voldoen (art. 5 lid 2 AVG).
Toetsing	O&P
VWN1 - ad hoc	a. Bij het ontwerpen, selecteren en gebruiken van toepassingen, diensten en producten wordt er nauwelijks of geen aandacht besteed aan de principes van Privacy by Design en Privacy by Default. b. Risicomanagement met betrekking tot privacy wordt sporadisch toegepast en stelt weinig tot geen eisen aan externe partijen.
VWN2 - herhaalbaar	a. Bij de ontwikkeling, implementatie en het gebruik van toepassingen, diensten en producten is er beperkte aandacht voor de implementatie van zowel Privacy by Design als Privacy by Default. De implementatie is gefragmenteerd en/of inconsistent. b. Wanneer externe partijen betrokken zijn, wordt er soms, in het kader van risicomanagement, naar hun privacy risicomanagement gevraagd, maar dit gebeurt niet systematisch of conform de principes van Privacy by Design. c. Toepassingen, diensten en producten zijn soms zodanig geconfigureerd dat alleen de strikt noodzakelijke persoonsgegevens worden verwerkt. Echter, dit gebeurt niet altijd en mist een begeleidend beleid of documentatie.
VWN3 - bepaald	a. In het kader van risicomanagement hanteert de organisatie gedocumenteerde eisen en beginselen voor zowel Privacy by Design als Privacy by Default. Dit omvat de ontwikkeling, het ontwerp, de selectie, en het gebruik van toepassingen, diensten en producten. b. Voorafgaand aan de inkoop of de ontwikkeling van toepassingen, diensten en producten vindt systematisch een beoordeling plaats van de privacyrisico's. Hierbij worden de benodigde maatregelen vastgesteld om de privacybeginselen uit art. 5 lid 1 AVG na te leven. c. Bij samenwerking met externe partijen stelt de organisatie consequent eisen op het gebied van Privacy by Design. d. Privacy by Default is consequent geïntegreerd als een standaard aspect van de configuratie voor toepassingen, diensten en producten waarin verwerking met een hoog risico plaatsvindt.

Wat	Beschrijving
	e. Er zijn gedocumenteerde richtlijnen opgesteld die betrekking hebben op zowel de verwerking als de bescherming van gegevens, waarbij de principes van Privacy by Default centraal staan.
VWN4 - beheerst	a. Privacy by Default is consequent geïntegreerd als een standaard aspect van de configuratie voor alle toepassingen, diensten en producten. b. De organisatie heeft zowel Privacy by Design als Privacy by Default specifiek ingebed in haar processen om privacyrisico's effectief te verminderen en te beheersen. Dit beleid wordt organisatiebreed toegepast. c. De organisatie stelt strikte eisen aan externe partijen voor het toepassen van adequaat privacy risicomanagement. Deze eisen worden periodiek gecontroleerd en, indien nodig, verbeterd. d. De privacy-risicobeoordeling is een integraal onderdeel van de ontwikkeling, het ontwerp, de selectie en het gebruik van toepassingen, diensten en producten. Hierbij worden alle toepassingen standaard geconfigureerd om alleen de strikt noodzakelijke persoonsgegevens te verwerken. e. Er wordt consequent en periodiek gecontroleerd of de toepassingen, diensten en producten aan deze privacy-standaarden voldoen. Afwijkingen van het beleid worden direct gecorrigeerd en/of gedocumenteerd volgens het principe "pas toe of leg uit".
VWN5 - geoptimaliseerd	a. De organisatie past haar processen proactief aan bij nieuwe/gewijzigde risico's. Deze aanpassingen kunnen voortkomen uit informatie verkregen door risicobeoordeling, gewijzigde inzichten naar aanleiding van de evaluatie van een datalek, wijzigingen in wet- en regelgeving, of andere relevante factoren. Bij deze updates worden de principes van zowel Privacy by Design als Privacy by Default consequent toegepast. b. Strikte eisen met betrekking tot privacyrisicomanagement, zowel voor Privacy by Design als Privacy by Default, zijn verankerd in de contractuele relaties van de organisatie. c. Het beleid voor Privacy by Default, in het bijzonder het minimaliseren van gegevensverwerking, wordt consequent toegepast in alle nieuwe en bestaande toepassingen, processen en systemen. Hierbij wordt proactief geanticipeerd op en gereageerd op veranderingen in het privacylandschap.
AVG-UAVG	AVG 25 lid 1
ISO 27701:2019	7.4
VNG 3.0	6.2 6.3
Norea PCF	• PBD01 • PBD02 • PBD03 • RMA05

PR.07 - Bewaren en vernietigen

Wat	Beschrijving
Domein	Processen
Categorie	Bewaar- en vernietigingsbeleid
Beschrijving risico	Het ontbreken van een bewaar- en vernietigingsbeleid en/of het negeren of niet goed implementeren van de selectielijsten voor onderwijsinstellingen (waar van toepassing) kan ertoe leiden dat persoonsgegevens niet tijdig of correct worden verwijderd of geanonimiseerd, kan de organisatie persoonsgegevens bewaren die niet langer noodzakelijk zijn voor de bedrijfsvoering of voor het uitvoeren van een wettelijke verplichting. Onnodig bewaarde persoonsgegevens kunnen worden verwerkt voor andere dan de oorspronkelijke doelen. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen als gevolg van hergebruik van persoonsgegevens voor andere dan de oorspronkelijke doelen. Voor de organisatie: • imago- of reputatieschade. • gebrek aan vertrouwen. • extra kosten ivm te nemen maatregelen om te voldoen aan AVG-verplichtingen waaronder de bescherming van de persoonsgegevens.
Beheerdoelstelling	Persoonsgegevens worden tijdig verwijderd of geanonimiseerd.
Toelichting	Op basis van de archiefwet dienen Nederlandse onderwijsorganisaties selectielijsten te hanteren waarin bewaartermijnen zijn vastgelegd. Voor universiteiten geldt de ‘Selectielijst Universiteiten en Universitair Medische Centra’. Voor hogescholen is er de ‘Selectielijst hogescholen’. Binnen het MBO wordt een selectielijst gehanteerd voor de openbare gezagstaken en een documentair structuurplan voor de overige taken. Deze selectielijsten kunnen als onderdeel van het beleid worden aangemerkt. In het beleid moet worden opgenomen welke gegevens verwijderd dienen te worden nadat de wettelijke bewaartermijnen is verstreken. Voor persoonsgegevens die niet in de selectielijst zijn opgenomen en waarvoor geen wettelijke bewaartermijnen gelden, zijn beleidsregels opgenomen. Het SURFaudit toetsingskader Privacy hanteert verwijderen als synoniem voor vernietigen. Wanneer de organisatie hiervan afwijkt, dient dit in de systematiek die in het beleid wordt beschreven voor vernietigen van persoonsgegevens terug te komen. De procedures zijn de toepassing van het beleid in een specifiek geval. Procedures hebben betrekking op een of meer concrete verwerkingen en stellen voor die verwerking eenduidig vast wat de bewaartermijn is of hoe deze kan worden bepaald. Het bewaarbeleid is ook van toepassing op logging en back-ups, voor zover deze persoonsgegevens bevatten. Zie ook de EDPS flyer over anonimiseren van data: • EDPS - anonimiseren
Toetsing	O&P
VWN1 - ad hoc	a. Er is geen vastgesteld beleid voor het verwijderen en anonimiseren van gegevens ('bewaarbeleid' of ‘vernietigingsbeleid’). b. Het verwijderen of anonimiseren van persoonsgegevens vindt niet, onregelmatig en/of inconsistent (bijvoorbeeld afhankelijk van individuen of incidenten) plaats.
VWN2 - herhaalbaar	a. Er is informeel beleid of beleid op decentraal niveau voor het verwijderen en/of anonimiseren van gegevens. b. Voor algemene, veelvoorkomende gevallen zijn er procedures voor het verwijderen van gegevens, maar voor meer specifieke gevallen ontbreken deze procedures.

Wat	Beschrijving
VWN3 - bepaald	a. Er is beleid vastgesteld voor het verwijderen en/of anonimiseren van gegevens. b. De processen om persoonsgegevens te verwijderen of te anonimiseren zijn gedocumenteerd. c. Persoonsgegevens die niet meer nodig zijn worden tijdig verwijderd of geanonimiseerd, conform het beleid. d. Waar noodzakelijk zijn specifieke procedures vastgesteld voor het verwijderen van gegevens, waarin is vastgesteld wat de toepasselijke bewaartermijn is en op welke wijze verwijdering plaats dient te vinden.
VWN4 - beheerst	a. Het beleid en de procedures voor het verwijderen en anonimiseren van gegevens worden consequent toegepast. b. Het beleid en de procedures voor het verwijderen en anonimiseren worden periodiek geëvalueerd en zo nodig aangepast. c. Het beleid besteedt aandacht aan het verwijderen/anonimiseren bij leveranciers (bijvoorbeeld SaaS applicaties of applicaties die anderszins persoonsgegevens verwerken). d. Periodiek wordt gecontroleerd of applicaties daadwerkelijk verwijderen of anonimiseren conform het bewaar- en vernietigingsbeleid. e. Waar mogelijk wordt het verwijderen of anonimiseren van persoonsgegevens geautomatiseerd uitgevoerd.
VWN5 - geoptimaliseerd	a. Het beleid en de procedures voor het verwijderen en anonimiseren van gegevens zijn volledig, transparant, en worden gezien als krachtige hulpmiddelen binnen de organisatie. b. Het is mogelijk een geautomatiseerd bewaar- en vernietigingsregime toe te passen op persoonsgegevens, bij voorkeur ook gekoppeld aan doelen. c. Deze geautomatiseerde systemen zijn volledig geïntegreerd in de operationele processen van de organisatie.
AVG-UAVG	AVG 5 lid 1 sub e c
ISO 27701:2019	7.4
VNG 3.0	2.5
Norea PCF	• PPO05 • DRE01 • DRE02 • DDA01 • DDA02 • ENC03

Organisatorische inbedding

OI.01 – FG

Wat	Beschrijving
Domein	Organisatorische inbedding
Categorie	Aanwijzing en positie functionaris gegevensbescherming
Beschrijving risico	Als de FG-rol niet correct of volledig is ingebed binnen de organisatie kan dit de effectiviteit van haar toezichthoudende taken verminderen, wat kan leiden tot een gebrek aan adequaat intern toezicht op de verwerking en bescherming van persoonsgegevens. Dit kan een directe impact hebben op het vermogen van de organisatie om de rechten en vrijheden van personen/betrokkenen te waarborgen. Daarnaast kan een ontoereikende inbedding van de FG-rol ertoe leiden dat betrokkenen hinder ondervinden bij het uitoefenen van hun rechten, zoals het recht op informatie en het recht op verwijdering van hun gegevens. Bovendien kan het leiden tot een gebrek aan bewustzijn over en kennis van de AVG binnen de organisatie. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen als gevolg van het ontbreken van onafhankelijk intern toezicht door de FG. Voor de organisatie: gebrek aan vertrouwen. dwangmaatregelen of boetes opgelegd door de toezichthouder.
Beheerdoelstelling	De organisatie heeft een functionaris gegevensbescherming (FG) aangesteld /aangewezen en zodanig onafhankelijk gepositioneerd dat deze effectief toezicht kan houden.
Toelichting	Zie o.a. de website van de AP over de positionering van de FG: • AP - positionering van de FG De FG kan op eigen initiatief audits (laten) uitvoeren. Het management kan ook zelf het initiatief tot een audit nemen en dit bijvoorbeeld opnemen in het overall auditplan van de organisatie. Dit ontslaat de FG overigens niet van zijn rol om onafhankelijk toezicht te houden.
Toetsing	O
VWN1 - ad hoc	a. Er is geen FG aangesteld of de aangewezen FG heeft onvoldoende middelen, tijd of ondersteuning voor het effectief uitoefenen van zijn of haar wettelijke taken. b. De rol en verantwoordelijkheden van de FG zijn niet gedefinieerd. c. De contactgegevens van de FG ontbreken en zijn niet (makkelijk) vindbaar. d. De FG is niet betrokken bij opleiding en bewustwordingsprogramma's.
VWN2 - herhaalbaar	a. Een FG is aangesteld, maar de taken van de FG zijn niet duidelijk omschreven en/of de rol van de FG is niet onafhankelijk (genoeg) gepositioneerd in de organisatie. b. De FG heeft beperkte tijd, middelen of ondersteuning (van het management) om zijn of haar taken te vervullen. c. De betrokkenheid van de FG bij opleiding en bewustwordingsprogramma's is minimaal en/of gebeurt ad hoc.
VWN3 - bepaald	a. De taken en verantwoordelijkheden van de FG zijn duidelijk omschreven en is onafhankelijk gepositioneerd binnen de organisatie. De FG ontvangt geen instructies met betrekking tot de uitvoering van zijn of haar taken. b. De FG heeft geen taken of verplichtingen die kunnen leiden tot een belangenconflict bij de uitvoering van hun taken als FG. c. De FG heeft voldoende tijd en middelen om zijn of haar taken effectief uit te voeren. d. Het proces voor het aannemen van een FG en het functieprofiel van de FG voldoen aan de eisen gesteld in artikel 37 lid 5 van de AVG. Voor lang zittende FG's, waarbij de

Wat	Beschrijving
	oorspronkelijke selectiecriteria niet meer beschikbaar zijn, wordt geadviseerd om de huidige competenties en kwalificaties van de FG te toetsen tegen de vereisten van artikel 37, lid 5 van de AVG. e. De FG wordt tijdig betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens waaronder advies bij iedere DPIA. f. Contactgegevens van de FG zijn actueel, beschikbaar, en makkelijk te vinden. g. De FG is betrokken bij opleiding en bewustwordingsprogramma's op het gebied van privacy. h. De FG stemt periodiek af met het hoogste management binnen de organisatie. i. De FG brengt rechtstreeks verslag uit aan het hoogste management doet over de naleving van de AVG door de organisatie.
VWN4 - beheerst	a. De organisatie heeft een gedocumenteerd proces om de aanstelling en het functioneren van de FG te waarborgen. Dit document bevat onder meer: • Een duidelijke beschrijving dat de FG afstemt met (een portefeuillehouder van) het hoogste bestuursorgaan, inclusief details over hoe en met welke frequentie deze afstemming plaatsvindt. • Een uitgewerkte rolbeschrijving met daarin een heldere beschrijving van de bevoegdheden, rechten (waaronder ontslagbescherming) en plichten van de FG. b. De FG voert periodiek zelfevaluaties uit en betrekt het management bij het verfijnen van de rol en positie. Indien uit de evaluatie blijkt dat de taken onduidelijk zijn of de rol niet goed is gepositioneerd, betrekt de FG het management om samen tot een oplossing te komen. c. De contactgegevens van de FG zijn niet alleen beschikbaar, maar worden ook proactief gecommuniceerd naar relevante partijen. d. De FG brengt periodiek verslag uit aan het bestuur over de naleving van de AVG door de organisatie.
VWN5 - geoptimaliseerd	a. Het bestuur neemt proactief het initiatief om de stand van zaken met betrekking tot de bescherming van persoonsgegevens in de organisatie, inclusief audits, met de FG te bespreken. b. De FG brengt regelmatig ongevraagd advies uit; het bestuur past deze adviezen toe of legt vast waarom daarvan afgeweken wordt. c. De aanstelling, verantwoordelijkheden, en middelen voor de FG zijn optimaal en worden continu verbeterd. d. De FG speelt een strategische rol in het ontwikkelen en leveren van opleiding en bewustwordingsprogramma's. e. De FG is betrokken bij opleiding en bewustwordingsprogramma's op het gebied van privacy.
AVG-UAVG	AVG 33 AVG 37 AVG 38 AVG 39
ISO 27701:2019	6.3.1.1
VNG 3.0	3.2 7.1
Norea PCF	• RRE04 • SCO01 • SCO04

OI.02 – Privacyteam

Wat	Beschrijving
Domein	Organisatorische inbedding
Categorie	Privacyorganisatie
Beschrijving risico	Het gebrek aan voldoende (juridische) kennis en ervaring binnen de organisatie met betrekking tot privacy en de bescherming van persoonsgegevens kan leiden tot verkeerde besluiten omtrent de bescherming van persoonsgegevens en resulteren in onrechtmatige verwerkingen en/of onvoldoende gegevensbescherming met als gevolg dat geen of onvoldoende bescherming van de vrijheden en rechten van personen/betrokkenen wordt geboden. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door verkeerde besluitvorming omtrent de bescherming van persoonsgegevens. Voor de organisatie: • onrechtmatige verwerkingen. • datalekken. • imago- of reputatieschade. • gebrek aan vertrouwen. • dwangmaatregelen of boetes opgelegd door de toezichthouder. • schadeclaims van gedupeerden. • hogere kosten door naderhand (reparatie-) maatregelen te moeten nemen.
Beheerdoelstelling	Er is – naast de FG - ruime (juridische) kennis en ervaring binnen de organisatie beschikbaar over bescherming van persoonsgegevens en relevante wet- en regelgeving.
Toelichting	Het is van belang dat de organisatie beschikt over een samenhangende aanpak van de bescherming van persoonsgegevens en de relevante wet- en regelgeving. Daarbij is het ook van belang en dat hiervoor binnen de organisatie voldoende (juridische) kennis en ervaring aanwezig is en is onderlinge afstemming met alle relevante stakeholders noodzakelijk. De standpunten van de organisatie kunnen afwijken van het advies van de FG. Voorbeelden van relevante stakeholders zijn de archivaris en management. De ruime (juridische) kennis en ervaring over bescherming van persoonsgegevens en relevante wet- en regelgeving (naast de FG) is veelal in de tweede lijn belegd bij privacy officers (privacyadviseurs). Voor grote organisaties wordt aanbevolen om, naast de noodzakelijke beschikbaarheid van ruime (juridische) kennis en ervaring over de bescherming van persoonsgegevens en relevante wet-en regelgeving, één of meerdere privacyambassadeurs / privacycoördinatoren beschikbaar te hebben die binnen hun organisatieonderdeel eenvoudige privacyvraagstukken kunnen oplossen of daarin kunnen adviseren. Deze privacyambassadeurs / coördinatoren hebben inzicht in privacygerelateerde ontwikkelingen binnen de organisatie, zoals wensen en zorgen van betrokkenen en collega's. Tijdens een periodiek privacyoverleg worden deze signalen besproken en waar nodig opgevolgd.
Toetsing	O
VWN1 - ad hoc	a. Er is geen of weinig (juridische) kennis over. b. Er is geen aanvullende privacyfunctionaris (of andere privacydeskundignaast de FG.
VWN2 - herhaalbaar	a. Er zijn één of enkele privacy officers (of adviseurs) die actief bijdragen aan het oplossen van (complexvraagstukken over privacy en de bescherming van persoonsgegevens. b. Er is incidenteel en/of informeel overleg en afstemming tussen de privacy- en informatiebeveiligingsfunctionarissen.

Wat	Beschrijving
VWN3 - bepaald	a. Er is een (virtueel) privacyteam waarbij de FG, privacy officer(s) en eventuele decentrale privacy ambassadeurs/coördinatoren zijn aangesloten. b. Het privacyteam werkt nauw samen met de informatiebeveiligingsfunctionarissen om vraagstukken rond informatiebeveiliging speelt, zoveel mogelijk gezamenlijk of althans in overleg, op te lossen. c. Medewerkers kunnen eenvoudig en makkelijk contact opnemen met het privacyteam. Het privacyteam reageert binnen een vooraf vastgestelde maximale reactietijd op vragen uit de organisatie. d. Het privacyteam heeft periodiek overleg om de werkzaamheden te bespreken en activiteiten af te stemmen, met betrokkenheid van relevante stakeholders.
VWN4 - beheerst	a. Privacy officer(s) en eventuele decentrale privacy ambassadeurs/-coördinatoren evalueren periodiek de privacygerelateerde werkzaamheden binnen de organisatie. De FG kan hier ook over adviseren. Daar waar nodig worden verbeteringen doorgevoerd.
VWN5 - geoptimaliseerd	a. Het initiatief tot verbeteringen van de privacygerelateerde werkzaamheden binnen de organisatie komt van de teams, afdelingen of het bestuur zelf in plaats van de privacyfunctionarissen. b. Organisatieonderdelen beschikken met betrekking tot de diensten die zij leveren over uitgebreide (juridische) kennis en ervaring over bescherming van persoonsgegevens en relevante wet- en regelgeving. c. Privacyfunctionarissen werken proactief samen met andere stakeholders voor de continue verbetering van de privacygerelateerde werkzaamheden.
AVG-UAVG	-
ISO 27701:2019	6.3
VNG 3.0	3.1
Norea PCF	• RRE04 • SC004 • LRC01

OI.03 – Betrokkenheid

Wat	Beschrijving
Domein	Organisatorische inbedding
Categorie	Betrokkenheid medezeggenschap
Beschrijving risico	Het niet of onvoldoende betrekken van het medezeggenschapsorgaan bij besluiten omtrent de bescherming van persoonsgegevens en het niet of onvoldoende informeren van de medezeggenschap kunnen leiden tot verlies van vertrouwen en draagvlak. Daarnaast kan het leiden tot een overtreding van de wettelijk vastgelegde rechten omtrent medezeggenschap. Bovendien beperkt het de mogelijkheid om inzichten over de bescherming van persoonsgegevens met het medezeggenschapsorgaan te kunnen delen met als doel om het beleid en procedures voor de bescherming van persoonsgegevens te kunnen optimaliseren. Dit kan leiden tot: Voor de organisatie: • gebrek aan vertrouwen. • dwangmaatregelen of boetes bij niet naleving wettelijke vereisten omtrent medezeggenschap.
Beheerdoelstelling	Het medezeggenschapsorgaan (MR/OR) wordt geïnformeerd en betrokken bij de omgang met en de bescherming van persoonsgegevens van medewerkers en onderwijsdeelnemers.
Toelichting	Medezeggenschap is in de sector onderwijs niet uniform geregeld. Voor het MBO geldt de Wet op de Ondernemingsraden (WOR) en voor HBO en WO de Wet op het Hoger Onderwijs en Wetenschappelijk Onderzoek (WHW). Als het om personeel gaat hebben de medezeggenschapsorganen in de hele sector instemmingsrecht op regelingen die de verwerking van persoonsgegevens van personeel betreffen. Voor regelingen die verwerking van persoonsgegevens van onderwijsdeelnemers (en eventueel overigen) is dat niet uniform geregeld. Het MBO heeft onderwijsdeelnemersraden voor de medezeggenschap van onderwijsdeelnemers. Deze onderwijsdeelnemersraad heeft instemmingsrecht op regelingen over de verwerking van persoonsgegevens van onderwijsdeelnemers. Voor HBO en WO is dit niet wettelijk geregeld en is vaak individueel per organisatie afgesproken of de medezeggenschap instemmingsrecht heeft of dat er enkel sprake is van een informatieplicht. Het is dus van belang om hiervoor vooraf de lokale regelingen te raadplegen of om dit te bespreken met de experts op dit terrein. Geraadpleegde bronnen: • open.overheid (pagina 9 alinea V) • Tweede Kamer (pagina 7 eerste rij)
Toetsing	O
VWN1 - ad hoc	a. Het medezeggenschapsorgaan wordt niet of slechts informeel betrokken bij onderwerpen over de omgang met en bescherming van persoonsgegevens.
VWN2 - herhaalbaar	a. Het medezeggenschapsorgaan wordt ad hoc betrokken bij onderwerpen over de omgang met en bescherming van persoonsgegevens. b. De informatievoorziening aan het medezeggenschapsorgaan is willekeurig en ongestructureerd.
VWN3 - bepaald	a. Er is een gedocumenteerd proces dat specificeert hoe en wanneer het medezeggenschapsorgaan geïnformeerd en betrokken wordt bij wettelijke taken op het gebied van privacy. b. Instemmingsprocedures zijn duidelijk gedocumenteerd en worden gevolgd waar wettelijk vereist.
VWN4 - beheerst	a. Het medezeggenschapsorgaan wordt actief geïnformeerd en qmunicatie daaromheen worden periodiek geëvalueerd en waar nodig aangepast.

Wat	Beschrijving
VWN5 - geoptimaliseerd	a. Er is een breed bewustzijn in de organisatie over de rol van het medezeggenschapsorgaan in de omgang met en bescherming van persoonsgegevens, en over de rol van overige relevante doelgroepen voor zover deze tot het mandaat van het medezeggenschapsorgaan behoren. b. Het medezeggenschapsorgaan is proactief betrokken, zowel op verzoek als ongevraagd, bij onderwerpen met betrekking tot de omgang met en bescherming van persoonsgegevens van medewerkers en andere relevante groepen binnen hun mandaat. c. De privacy aanspreekpunten in de organisatie en het medezeggenschapsorgaan weten elkaar makkelijk te bereiken. Hier wordt bijvoorbeeld aandacht aan gegeven in o.a. privacy awareness trainingen en de rol van het medezeggenschapsorgaan.
AVG-UAVG	-
ISO 27701:2019	6.3
VNG 3.0	3.3
Norea PCF	

OI.04 – Bewustwording

Wat	Beschrijving
Domein	Organisatorische inbedding
Categorie	Bewustwording
Beschrijving risico	Een gebrek aan bewustwording bij medewerkers en onderwijsdeelnemers met betrekking tot de bescherming van persoonsgegevens welke tot doel heeft dat zij hun verantwoordelijkheden kennen en hun taken goed uit kunnen voeren, kan ertoe leiden dat verkeerde besluiten worden genomen hetgeen de kans op onrechtmatige verwerking, verlies of misbruik van persoonsgegevens vergroot. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door verkeerde besluitvorming omtrent de bescherming van persoonsgegevens Voor de organisatie: • onrechtmatige verwerkingen. • datalekken. • imago- of reputatieschade. • gebrek aan vertrouwen. • dwangmaatregelen of boetes opgelegd door de toezichthouder. • schadeclaims van gedupeerden.
Beheerdoelstelling	Medewerkers en onderwijsdeelnemers worden bewust gemaakt van privacy gerelateerde kwesties en hun verantwoordelijkheden met betrekking tot het beschermen van persoonsgegevens. Ook zijn er voldoende middelen beschikbaar om medewerkers te trainen.
Toelichting	Met "medewerkers" worden ook ZZP'ers en externe medewerkers bedoeld, zodat zij eveneens geïnformeerd worden over privacy gerelateerde kwesties en hun verantwoordelijkheden met betrekking tot het beschermen van persoonsgegevens. Denk in dit verband ook aan onderwijsdeelnemers die meewerken in onderzoeken en bij activiteiten/events. Ook overige onderwijsdeelnemers worden op passende wijze geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens en wat zij zelf op dit gebied kunnen doen, aangezien onderwijsdeelnemers ook datalekken kunnen veroorzaken. Dit kan variëren van formele informatiesessies, inbedding in het curriculum tot informele discussiesessies, afhankelijk van wat het meest geschikt is voor de betreffende organisatie.
Toetsing	O&P
VWN1 - ad hoc	a. Er zijn geen activiteiten of initiatieven gedefinieerd of uitgevoerd om het bewustzijn over privacy te vergroten. Medewerkers worden bij indiensttreding niet geïnformeerd over privacy. b. Onderwijsdeelnemers worden niet geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens.
VWN2 - herhaalbaar	a. Er zijn activiteiten of initiatieven gedefinieerd om het bewustzijn over privacy te vergroten, maar deze worden informeel uitgevoerd (alleen op verzoek of als reactie op een geïdentificeerde behoefte, bijvoorbeeld naar aanleiding van een incident). b. Onderwijsdeelnemers worden op incidentele basis geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens.
VWN3 - bepaald	a. Er is een programma/opleidingsplan waarin medewerkers bij indiensttreding en, indien nodig, tijdens het dienstverband worden geïnformeerd over privacy en de bescherming van persoonsgegevens. b. Medewerkers zijn goed geïnformeerd over hun verantwoordelijkheden met betrekking tot privacy en de bescherming van persoonsgegevens en handelen daarnaar. c. Onderwijsdeelnemers worden op een planmatige manier geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens.

Wat	Beschrijving
VWN4 - beheerst	a. Voor alle niveaus worden de vaardigheidsvereisten systematisch bijgehouden; deskundigheidsbevordering is gewaarborgd in alle kritieke gebieden en certificering op het gebied van privacyskills wordt aangemoedigd. b. Periodiek wordt geëvalueerd of met de trainingen de beoogde resultaten worden behaald en waar nodig worden trainingen en of het trainingsprogramma aangepast. c. Medewerkers en ingehuurde medewerkers hebben aantoonbaar een passende (bewustwordings)training of instructie gevolgd over hun verantwoordelijkheden met betrekking tot de bescherming van persoonsgegevens.
VWN5 - geoptimaliseerd	a. Er is een formeel proces dat zich richt op voortdurende vaardigheidsverbetering, gebaseerd op heldere persoonlijke en organisatiebrede doelen, en waarbij medewerkers en onderwijsdeelnemers geïnformeerd worden over relevante privacygerelateerde kwesties. b. Privacybewustzijn en de bescherming van persoonsgegevens zijn volledig geïntegreerd in alle aspecten van de organisatie, met volledige betrokkenheid en participatie van alle medewerkers, inclusief het hoogste management. c. Onderwijsdeelnemers worden consequent geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens. Deze informatie is geïntegreerd in het onderwijsprogramma, waarbij onderwijsdeelnemers actief betrokken zijn en participeren.
AVG-UAVG	AVG 39 1b AVG 24 lid 1
ISO 27701:2019	6.4.2.2
VNG 3.0	3.4
Norea PCF	• SCO02 • SCO03 • RRE05 • SAT01 • SAT02 • SAT03 • SCO02

Rechten van betrokkenen

RB.01 - Rechten van betrokkenen

Wat	Beschrijving
Domein	Rechten van betrokkenen
Categorie	Afhandeling rechten van betrokkenen
Beschrijving risico	Het ontbreken van passende procedures voor de afhandeling van de rechten van betrokkenen kan leiden tot inefficiënte en onnauwkeurige verwerking van verzoeken. Dit kan resulteren in vertragingen bij het beantwoorden van verzoeken, het niet correct uitvoeren van de rechten van betrokkenen en het niet naleven van wettelijke verplichtingen. Onvoldoende duidelijkheid en communicatie naar betrokkenen kan verwarring en onzekerheid veroorzaken. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door onvolledige of trage afhandeling van de rechten van betrokkene Voor de organisatie: • imago- of reputatieschade. • gebrek aan vertrouwen. • schadeclaims van gedupeerden.
Beheerdoelstelling	De organisatie heeft een procedure voor de afhandeling van rechten van betrokkenen waarin de technische en organisatorische maatregelen zijn vastgelegd en wie verantwoordelijk is om deze uit te voeren.
Toelichting	Verzoeken worden bij voorkeur op dezelfde manier afgehandeld als waarop ze zijn ingediend. Wanneer de betrokkene zijn verzoek elektronisch indient, wordt de informatie indien mogelijk elektronisch verstrekt, tenzij de betrokkene anderszins verzoekt (art 12 lid 3).
Toetsing	O&P
VWN1 - ad hoc	a. De organisatie heeft geen technische of organisatorische maatregelen genomen om de rechten van betrokkenen te waarborgen. b. Er is geen proces voor het indienen en afhandelen van verzoeken. c. Medewerkers herkennen AVG-verzoeken niet en weten niet naar wie ze deze moeten doorsturen voor afhandeling. d. De organisatie houdt geen registratie bij van eerder behandelde verzoeken. Er bestaat geen procedure om, ten behoeve van consistentie en de waarborg van rechtsgelijkheid, nieuwe verzoeken te toetsen aan de hand van eerder afgehandelde verzoeken.
VWN2 - herhaalbaar	a. De organisatie heeft voor de afhandeling van rechten van betrokkenen enkele technische en organisatorische maatregelen genomen, maar de implementatie is onvolledig en inconsistent. b. Verzoeken kunnen zowel analoog als digitaal worden ingediend, maar de communicatie hierover is gebrekkig. c. Er zijn basisprocedures voor de afhandeling van verzoeken, maar de naleving van termijnen is inconsistent en/of de communicatie met betrokkenen is gebrekkig. d. Er is een registratie van eerder behandelde verzoeken, maar deze wordt niet consequent gebruikt om, ten behoeve van consistentie en de waarborg van rechtsgelijkheid, nieuwe verzoeken te toetsen.
VWN3 - bepaald	a. Er is een procedure voor de afhandeling van verzoeken van betrokkenen vastgesteld, waarin ten minste het volgende is opgenomen: • op welke wijze verzoeken kunnen worden ingediend; • op welke wijze de identiteit van verzoeker wordt vastgesteld;

Wat	Beschrijving
	• wie verantwoordelijk is voor de afhandeling; • de toepasselijke termijnen; • de criteria voor het toewijzen en afwijzen van een verzoek; • het informeren van ontvangers over een verzoek. b. Verzoeken kunnen zowel analoog als digitaal worden ingediend en dit proces is duidelijk gecommuniceerd naar betrokkenen. c. Betrokkenen ontvangen altijd een ontvangstbevestiging van hun verzoeken en worden tijdig geïnformeerd over de status van de behandeling. d. Applicaties en systemen bevatten voldoende mogelijkheden om de rechten van betrokkenen effectief uit te voeren. e. Er is een registratie van eerder behandelde verzoeken die consequent wordt bijgehouden en gebruikt om nieuwe verzoeken te beoordelen, met als doel de rechtsgelijkheid te waarborgen. f. Medewerkers zijn goed getraind in het herkennen van AVG-verzoeken en weten precies naar wie ze deze moeten doorsturen.
VWN4 - beheerst	1. Verzoeken van betrokkenen worden tijdig afgehandeld en er is een proces voor het signaleren, melden en analyseren van vertragingen. a. Er is een duidelijke procedure voor de afhandeling van verzoeken, inclusief monitoring en verbetering van de reactietijden. Dit wordt periodiek geanalyseerd om verbetermaatregelen te treffen. b. De organisatie houdt een gedetailleerde registratie bij van eerder behandelde verzoeken en gebruikt deze om nieuwe verzoeken consistent en nauwkeurig te toetsen.
VWN5 - geoptimaliseerd	1. Alle applicaties en systemen bevatten geavanceerde en effectieve mogelijkheden voor de uitvoering van de rechten van betrokkenen. a. Er worden benchmarks (bijvoorbeeld binnen de onderwijssector) uitgevoerd om te toetsen of de uitvoering van rechten van betrokkenen aansluit op wat algemeen gangbaar is.
AVG-UAVG	AVG 12 AVG 15 AVG 16 AVG 17 AVG 18 AVG 19 AVG 21 UAVG 44
ISO 27701:2019	7.3
VNG 3.0	4.2
Norea PCF	• DAR01 • DAR03 • DAR04 • DCR01 • DCR03 • DCR04 • DDR01 • DDR02 • DDR04 • URE02

RB.02 – Informatieplicht

Wat	Beschrijving
Domein	Rechten van betrokkenen
Categorie	Informatieplicht
Beschrijving risico	Het niet vooraf informeren van betrokkenen over gegevensverwerking kan leiden tot een gebrek aan transparantie en kan de organisatie niet of niet voldoende verantwoorden dat de gegevensverwerking voldoet aan de beginselen van behoorlijke en transparante verwerking. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door een gebrek aan informatie over de verwerking van zijn/haar persoonsgegevens. Voor de organisatie: • imago- of reputatieschade. • gebrek aan vertrouwen. • schadeclaims van gedupeerden.
Beheerdoelstelling	Betrokkenen worden, zoveel als mogelijk, voorafgaand aan een verwerking op de hoogte gesteld van de wettelijk vereiste informatie over de verwerking van hun persoonsgegevens.
Toelichting	Geadviseerd wordt om de privacyverklaring te ondersteunen met een verwijzing naar een online gepubliceerd verwerkingsregister. Zorg er bij het publiceren van het verwerkingsregister voor dat: namen van eigenaren van verwerkingen zijn verwijderd, er niet op andere wijze gevoelige of aan personen te relateren informatie wordt gepubliceerd, er geen gevoelige informatie over informatiebeveiliging C31 van de organisatie wordt prijsgegeven. Het publiceren van het register is niet verplicht. De privacyverklaring moet deze criteria en onderwerpen bevatten: • de identiteit van de verwerkingsverantwoordelijke; • contactgegevens van de FG; • verwerkingsdoeleinden en rechtsgrond; • de betrokken categorieën van persoonsgegevens; • eventuele ontvangers van persoonsgegevens; • informatie over doorgifte naar landen buiten de EER; • bewaartermijn; • rechten van de betrokkene; • de mogelijkheid om verstrekte toestemming in te trekken; • mogelijkheid om klacht in te dienen bij AP; • het bestaan van geautomatiseerde besluitvorming en profilering. • de bron waar de persoonsgegevens vandaan komen • gevolgen als gegevens niet worden verstrekt. De informatie moet beknopt, transparant en begrijpelijk zijn. Vermijd jargon zoveel mogelijk. Bezoekers op de website moeten volgens wet- en regelgeving transparante informatie krijgen over het gebruik van cookies. Het advies is om dit vast te leggen in een cookiebeleid.
Toetsing	O&P
VWN1 - ad hoc	a. Betrokkenen worden niet of onvoldoende geïnformeerd over hun rechten. b. Er is geen informatie verstrekt aan betrokkenen van wie de persoonsgegevens niet rechtstreeks zijn verkregen. c. De organisatie heeft geen algemene privacyverklaring gepubliceerd op de website of in applicaties en formulieren. d. Er is geen cookiebeleid of uniforme afspraken over de toepassing van cookies. e. Bezoekers van de website worden niet geïnformeerd over het gebruik van cookies.
VWN2 - herhaalbaar	a. Betrokkenen worden geïnformeerd, maar de communicatie is soms niet adequaat of te laat.

Wat	Beschrijving
	b. Er is een algemene privacyverklaring, maar deze is mogelijk niet volledig of niet up-to-date, en is niet in eenvoudige en duidelijke op de doelgroep gerichte taal opgeschreven. c. De informatie over de verwerking van persoonsgegevens in applicaties en formulieren is beperkt en niet altijd duidelijk. d. Betrokkenen van wie de persoonsgegevens niet rechtstreeks zijn verkregen, worden niet altijd of niet volledig geïnformeerd. e. Er zijn informele afspraken over het gebruik van cookies, maar deze voldoen niet (volledig) aan wet-en regelgeving en/of niet consequent geïmplementeerd.
VWN3 - bepaald	a. Er is beleid vastgesteld over het informeren van betrokkenen, inclusief de timing van de informatieverstrekking. b. Betrokkenen worden adequaat en tijdig geïnformeerd in overeenstemming met de beginselen van behoorlijke en transparante verwerking. c. Personen van wie de persongsgegevens niet rechtstreeks zijn verkregen, worden binnen een maand geïnformeerd. d. De organisatie heeft een privacyverklaring op de algemene website in eenvoudige en duidelijke taal (taalniveau B1) en een verwijzing in applicaties en formulieren waar verwerkingen plaatsvinden. e. Er is cookiebeleid vastgelegd en dit voldoet aan wet- en regelgeving. f. De website informeert gebruikers over het cookiebeleid.
VWN4 - beheerst	a. Er wordt periodiek geëvalueerd of de procedures voor het informeren van betrokkenen adequaat zijn en worden nagekomen. Daar waar nodig worden aanpassingen doorgevoerd. b. De privacyverklaring is up-to-date en de inhoud wordt afgestemd op de specifieke context van applicaties en formulieren. c. Het cookiebeleid en de implementatie ervan worden periodiek geëvalueerd. Daar waar nodig worden aanpassingen doorgevoerd.
VWN5 - geoptimaliseerd	a. Transparantie wordt beschouwd als een kwaliteitsaspect en kans voor de organisatie om aan te tonen hoe zorgvuldig ze omgaat met persoonsgegevens van onderwijsdeelnemers, medewerkers en overige betrokkenen. Er is bijvoorbeeld een online gepubliceerd verwerkingsregister. b. Applicaties en formulieren bieden uitgebreide uitleg over de verwerking van persoonsgegevens. c. Er is een proactieve benadering om de gebruikerservaring van de website met betrekking tot de bescherming van persoonsgegevens te verbeteren, inclusief een transparant en begrijpelijk cookiebeleid. d. Het cookiebeleid en de implementatie ervan worden proactief getoetst aan de nieuwste inzichten en richtlijnen.
AVG-UAVG	AVG 12 AVG 13 grond 60, 61 en 62 AVG 14 AVG 15
ISO 27701:2019	7.3
VNG 3.0	4.1
Norea PCF	• PST01

RB.03 – Toestemming

Wat	Beschrijving
Domein	Rechten van betrokkenen
Categorie	Toestemming
Beschrijving risico	Indien de organisatie niet voldoet aan de voorwaarden voor toestemming zoals beschreven in artikel 7 en 8 van de AVG, kan de verleende toestemming niet als vrijelijk gegeven beschouwd worden, mogelijk ongeldig zijn en dat persoonsgegevens onrechtmatig worden verwerkt. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door het ontbreken van toestemming in overeenstemming met de artikelen 7 en 8 van de AVG. Voor de organisatie: • onrechtmatige verwerkingen. • imago- of reputatieschade. • gebrek aan vertrouwen. • dwangmaatregelen of boetes opgelegd door de toezichthouder. • schadeclaims van gedupeerden.
Beheerdoelstelling	De organisatie voldoet aan de wettelijke vereisten wanneer een verwerking is gebaseerd op toestemming.
Toelichting	De grondslag (toestemming) behoort te worden geregistreerd in het verwerkingsregister. Toestemmingsverklaringen moeten zodanig worden gedocumenteerd dat aangetoond kan worden dat betrokkene toestemming heeft verleend. Bij verwerkingen die zijn gebaseerd op toestemming wordt toestemming gevraagd in een gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal. De betrokkene stemt toe door middel van een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting in de vorm van een verklaring of een ondubbelzinnige actieve handeling. Indien het gaat om toestemming voor het gebruik van persoonsgegevens van personen onder de 16 jaar (bij jonge onderwijsdeelnemers of proefpersonen voor onderzoek), dan dient de toestemming van de ouders of voogd(en) te worden vastgelegd. Jongeren tussen 12 en 16 jaar kunnen een door hun ouders / vertegenwoordigers gegeven toestemming intrekken en zelf hun rechten uitoefenen. Zorg dat de organisatie bij het vragen van toestemming voldoet aan de informatieplicht.
Toetsing	O&P
VWN1 - ad hoc	a. Er zijn geen gestandaardiseerde processen voor de identificatie van verwerkingen die op toestemming zijn gebaseerd. b. Er is geen documentatie van toestemming c. Er is geen procedure om toestemming in te trekken.
VWN2 - herhaalbaar	a. De organisatie heeft een informeel proces om verwerkingen die op toestemming zijn gebaseerd te identificeren, maar dit proces wordt niet consequent gevolgd. b. De organisatie vraagt toestemming van betrokkenen, maar de toestemming is niet altijd vrij, geïnformeerd, specifiek en ondubbelzinnig. c. Toestemming wordt in een aantal gevallen gedocumenteerd, maar dit is nog niet consequent of volledig. d. Betrokkenen hebben de mogelijkheid om toestemming in te trekken, maar dit proces is niet altijd duidelijk of gemakkelijk.
VWN3 - bepaald	a. De organisatie heeft vastgesteld welke verwerkingen op toestemming zijn gebaseerd.

Wat	Beschrijving
	b. Toestemming wordt correct gevraagd volgens de vereisten die zijn opgenomen in AVG artikel 4, grond 32, 33, 42, en 43. c. Toestemming wordt consequent en volledig gedocumenteerd. d. Betrokkenen kunnen hun toestemming gemakkelijk intrekken.
VWN4 - beheerst	a. De organisatie evalueert periodiek haar processen om te bepalen welke verwerkingen op toestemming zijn gebaseerd. b. Er zijn periodieke beoordelingen en audits om ervoor te zorgen dat toestemming correct wordt gevraagd en gedocumenteerd. c. Het proces voor het intrekken van toestemming wordt periodiek geëvalueerd en indien nodig aangepast.
VWN5 - geoptimaliseerd	a. De organisatie heeft systemen en processen om te bepalen welke verwerkingen op toestemming zijn gebaseerd. b. Documentatie van toestemming wordt (automatisch) bijgewerkt en gevolgd via systemen. c. Betrokkenen kunnen hun toestemming gemakkelijk intrekken en intrekkingen worden tijdig verwerkt.
AVG-UAVG	AVG 4 sub 11 AVG 6 lid 1 sub a; AVG 7; AVG 8 AVG 9 lid 2 sub a in relatie tot AVG 6 (en 9): UAVG art 5 UAVG 22 UAVG 24 UAVG 25 UAVG 26 UAVG 27 UAVG 28 UAVG 30
ISO 27701:2019	7.2 7.3
VNG 3.0	4.3
Norea PCF	• CFR02 • CFR03 • CFR04

RB.04 - Geautomatiseerde besluitvorming

Wat	Beschrijving
Domein	Rechten van betrokkenen
Categorie	Geautomatiseerde individuele besluitvorming waaronder profilering (Geautomatiseerde besluitvorming en/of profilering)
Beschrijving risico	Het niet voldoen aan de wettelijke vereisten voor geautomatiseerde besluitvorming en/of profilering kan de bescherming van de privacy van betrokkenen in gevaar brengen. Een tekort aan begrip, documentatie en waarborgen kan leiden tot onbedoelde gevolgen, discriminatie of beslissingen met een mogelijk rechtsgevolg dat de betrokkene in aanmerkelijke mate treft, zoals vastgelegd in artikel 22, lid 1 van de AVG. Het adequaat informeren van betrokkenen over dergelijke besluitvorming is cruciaal om aan deze wettelijke verplichtingen te voldoen en de privacy van betrokkenen te beschermen. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door verkeerde besluitvorming omtrent de bescherming van persoonsgegevens. Voor de organisatie: • onrechtmatige verwerkingen. • imago- of reputatieschade. • gebrek aan vertrouwen. • dwangmaatregelen of boetes opgelegd • door de toezichthouder. • schadeclaims van gedupeerden.
Beheerdoelstelling	De organisatie voldoet aan de wettelijke vereisten voor geautomatiseerde individuele besluitvorming, waaronder profilering.
Toelichting	Als geautomatiseerde besluitvorming en/of profilering wordt toegepast, wordt geadviseerd om een procedure te implementeren waarin is opgenomen: • welke informatie en uitleg aan de betrokkene moet worden verstrekt over het geautomatiseerde besluitvormingsproces; • op welke manier de betrokkene de mogelijkheid heeft om zijn standpunt kenbaar te maken en besluiten aan te vechten; • hoe in specifieke gevallen menselijke tussenkomst wordt geboden. Beheersing van geautomatiseerde besluitvorming is essentieel (maatschappelijk onder hoge aandacht). Zie voor de VWN4.2 genoemde AI-act onder andere: • EURLEX • Europees Parlement • AP inzet AI Act
Toetsing	O&P
VWN1 - ad hoc	a. Er is niet of onvoldoende bekend of er geautomatiseerde individuele besluitvorming en/of profilering binnen de organisatie plaatsvindt. b. Betrokkenen worden niet of nauwelijks geïnformeerd over geautomatiseerde individuele besluitvorming en/of profilering.
VWN2 - herhaalbaar	a. Er is (enigszins) bekend dat binnen de organisatie gebruik maakt van geautomatiseerde individuele besluitvorming en/of profilering, maar de organisatie heeft geen of beperkt begrip van de gebruikte algoritmes en/of er is geen of onvolledige documentatie hierover. b. DPIA's worden niet consequent voor elke nieuwe of gewijzigde geautomatiseerde individuele besluitvorming en/of profilering uitgevoerd. c. Betrokkenen worden op ad hoc basis geïnformeerd over deze vorm van besluitvorming. d. Er zijn informele procedures voor het omgaan met geautomatiseerde besluitvorming en/of profilering waaronder de mogelijkheid voor betrokkenen om hun standpunt kenbaar te maken en besluiten aan te vechten.

Wat	Beschrijving
VWN3 - bepaald	a. De organisatie heeft een volledig begrip van en documentatie, waaronder een algoritmeregister, over welke processen gebruik maken van (gedeeltelijk) geautomatiseerde individuele besluitvorming en/of profilering. b. Er zijn formele procedures geïmplementeerd voor geautomatiseerde besluitvorming en/of profilering, inclusief het informeren van betrokkenen en het bieden van mogelijkheden voor betrokkenen om hun standpunt kenbaar te maken en besluiten aan te vechten. c. Betrokkenen worden geïnformeerd over geautomatiseerde besluitvorming en/of profilering op een wijze die in overeenstemming is met de informatieplicht. d. Er wordt een DPIA uitgevoerd voor elke nieuwe geautomatiseerde besluitvorming en/of profilering.
VWN4 - beheerst	a. Geautomatiseerde besluiten en/of profilering, worden periodiek geëvalueerd. b. Periodiek worden gerelateerde DPIA's geëvalueerd. Daar waar nodig worden de privacy waarborgen verbeterd. c. De organisatie voert periodiek audits uit om te controleren of de processen van geautomatiseerde individuele besluitvorming en/of profilering voldoen aan de AVG-vereisten en andere wettelijke vereisten, zoals de AI Act. d. De organisatie communiceert proactief informatie over deze vorm van besluitvorming aan betrokkenen.
VWN5 - geoptimaliseerd	a. Er is een (interne) tool waarmee geautomatiseerde besluiten en/of profilering, eenvoudig kunnen worden bijgehouden en geëvalueerd op juistheid. b. De organisatie voorziet belanghebbenden van actuele informatie op basis waarvan automatische besluitvorming plaatsvindt. c. De organisatie past continu DPIA's toe op geautomatiseerde besluitvorming en/of profilering, waarbij de resultaten worden gebruikt om processen te verbeteren.
AVG-UAVG	AVG 22 UAVG 40
ISO 27701:2019	7.4
VNG 3.0	4.4
Norea PCF	• DAR01 • PIA01

Samenwerking

SW.01 - Externe AVG-rollen

Wat	Beschrijving
Domein	Samenwerking
Categorie	AVG-rollen
Beschrijving risico	Wanneer een organisatie geen duidelijkheid heeft over de AVG-rollen (zoals verwerkingsverantwoordelijke, verwerker of gezamenlijk verwerkingsverantwoordelijken daarover geen formele afspraken maakt met partijen die betrokken zijn bij de verwerking van persoonsgegevens, kunnen verantwoordelijkheden zoals vastgelegd in art. 26, 28, 29 en 32 AVG onvoldoende worden erkend en belegd. Dit kan tot gevolg hebben dat persoonsgegevens onrechtmatig worden doorgegeven, onrechtmatig (verder) worden verwerkt en er een gebrek aan verantwoordelijkheid en controle ontstaat. Met name bij het niet toepassen van artikel 26 AVG kan dit betekenen dat respectieve verantwoordelijkheden en verplichtingen, vooral met betrekking tot de rechten van betrokkenen, niet duidelijk zijn vastgelegd. Hierdoor weten betrokkenen niet bij wie zij terecht kunnen voor hun rechten en verplichtingen. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door een gebrek aan verantwoordelijkheid en controle. Voor de organisatie: • onrechtmatige verwerking. • imago- of reputatieschade. • dwangmaatregelen of boetes opgelegd door de toezichthouder. • schadeclaims van gedupeerden.
Beheerdoelstelling	De organisatie heeft de AVG-rol voor alle betrokken partijen die persoonsgegevens verwerken inzichtelijk en heeft conform de AVG met deze partijen afspraken gemaakt.
Toelichting	Denk bij betrokken partijen aan de verwerking van persoonsgegevens door externe partijen in zowel onderwijs, onderzoek als bedrijfsvoering, maar ook in samenwerkingsverbanden, (data-)uitwisselingen. De organisatie is niet in alle gevallen (alleen) verwerkingsverantwoordelijke. In dat geval kan sprake zijn van gezamenlijke verantwoordelijkheid. Soms wordt verantwoordelijkheid ook overgedragen. Denk bijvoorbeeld aan gegevens die naar de belastingdienst gaan. Daarnaast eigenen sommige externe partijen zich (voor een deel van de gegevens) de rol van verwerkingsverantwoordelijke toe, bijvoorbeeld met het doel om hun dienstverlening te verbeteren. Dit dient ingeperkt te worden via de verwerkersovereenkomst.
Toetsing	O
VWN1 - ad hoc	a. De organisatie heeft de AVG-rollen van de organisatie zelf en die van externe partijen die betrokken zijn bij verwerking van persoonsgegevens niet inzichtelijk gemaakt. b. Voorafgaand aan een verwerking voert de organisatie geen beoordeling uit om te bepalen of een externe optreedt als gegevensverwerker, gezamenlijke verwerkingsverantwoordelijke of zelfstandige verwerkingsverantwoordelijke. c. Er worden geen of nauwelijks afspraken gemaakt met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken
VWN2 - herhaalbaar	a. Medewerkers hebben beperkt bewustzijn van het belang van het onderscheiden van AVG-rollen. b. De organisatie heeft de AVG-rollen van de organisatie en die van externe partijen deels inzichtelijk gemaakt, maar dit is gefragmenteerd en inconsistent. c. Er wordt incidenteel een beoordeling uitgevoerd om te bepalen of de externe partij optreedt als gegevensverwerker, gezamenlijke verwerkingsverantwoordelijke, of

Wat	Beschrijving
	zelfstandige verwerkingsverantwoordelijke, maar dit gebeurt niet systematisch en is sterk afhankelijk van individuen of afdelingen. d. Er worden in sommige gevallen afspraken gemaakt met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken, maar dit is niet uniform. e. Bij het gebruik van externe verwerkers is er onvoldoende inzicht in de inzet van subverwerkers en de afspraken die met hen zijn gemaakt
VWN3 - bepaald	a. De organisatie heeft de AVG-rollen van de organisatie en die van externe partijen duidelijk en inzichtelijk gemaakt en medewerkers zijn zich bewust van het belang om AVG-rollen te onderscheiden. b. Er is een gestandaardiseerd proces om voorafgaand aan elke gegevensverwerking te beoordelen en vast te stellen of de externe partij optreedt als gegevensverwerker, gezamenlijke verwerkingsverantwoordelijke, of zelfstandige verwerkingsverantwoordelijke. c. Er worden consistent afspraken gemaakt met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken. De overeenkomsten bevatten de elementen die in de AVG artikel 28 lid 3 zijn voorgeschreven en afspraken hoe wijzigingen (bijvoorbeeld wijziging van subverwerkers) worden gemeld. d. Het beheer van overeenkomsten met verwerkers, zelfstandig verwerkingsverantwoordelijken en gezamenlijke verwerkingsverantwoordelijken is adequaat belegd binnen de organisatie.
VWN4 - beheerst	a. AVG-rollen van externe partijen worden periodiek geëvalueerd.Indien noodzakelijk worden beleid en procedures aangepast. b. Naleving van de afspraken die zijn gemaakt met verwerkers en gezamenlijke verwerkingsverantwoordelijken wordt periodiek getoetst of geaudit. c. De afspraken met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken worden periodiek geëvalueerd en aangepast indien nodig. d. Het beheer en evaluatie van overeenkomsten met verwerkers, zelfstandig verwerkingsverantwoordelijken en gezamenlijke verwerkingsverantwoordelijken is goed georganiseerd en wordt periodiek geëvalueerd en waar nodig aangepast. e. Training en bewustwording over AVG-rollen zijn geïntegreerd in de processen en procedures van de organisatie.
VWN5 - geoptimaliseerd	a. Er is een eenvoudig en toegankelijk tool/systeem dat een overzicht/rapportages biedt van de AVG-rollen van externe partijen. b. De organisatie is in staat om snel en effectief te reageren op veranderingen in AVG-rollen van externe partijen, en past procedures en overeenkomsten dienovereenkomstig aan.
AVG-UAVG	AVG 26 AVG 28
ISO 27701:2019	7.2
VNG 3.0	5.
Norea PCF	• RRE01 • RRE03

SW.02 - Eenmalige verstrekkingen

Wat	Beschrijving
Domein	Samenwerking
Categorie	Toetsing gegevensverstrekking aan derden
Beschrijving risico	Het ontbreken van een uniform toetsingskader voor gegevensversterking aan derden en/of een systematische beoordeling daarvan waardoor gegevens mogelijk onrechtmatig en/of ongeautoriseerd aan derden worden verstrekt. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door onrechtmatige gegevensverstrekking. Voor de organisatie: • onrechtmatige verwerking. • imago- of reputatieschade. • dwangmaatregelen of boetes opgelegd door de toezichthouder. • schadeclaims van gedupeerden.
Beheerdoelstelling	De organisatie toetst ieder voornemen om persoonsgegevens aan een derde partij te verstrekken aan de relevante wet- en regelgeving.
Toelichting	Gegevensverstrekking aan derden dient gedocumenteerd te worden. Ten minste de volgende informatie dient te worden vastgelegd: • gegevens over de ontvanger. • de categorieën van persoonsgegevens. • de doeleinden. • de rechtsgrond voor verstrekking.
Toetsing	O&P
VWN1 - ad hoc	a. De organisatie heeft geen eenduidige, gestandaardiseerde procedure vastgesteld voor de toetsing van gegevensverstrekking aan derden. b. Het delen van persoonsgegevens met externe partijen gebeurt zonder voorafgaande toetsing of er is weinig tot geen bewustzijn van het belang van deze toetsing.
VWN2 - herhaalbaar	a. De organisatie voert sporadisch en ongestructureerd toetsingen uit op voorgenomen gegevensverstrekking aan externe partijen, zonder een systematische benadering en in overeenstemming met de toepasselijke (privacy)wetgeving. b. Een coherente, organisatiebrede procedure ontbreekt, wat leidt tot inconsistenties en variatie in de kwaliteit van de toetsingen. c. Relevante medewerkers (zoals inkoop, juridische afdeling, onderzoekers) hebben beperkt bewustzijn van het belang van het toetsen van de gegevensverstrekking aan externe partijen.
VWN3 - bepaald	a. De organisatie heeft een uniform, organisatiebreed kader geïmplementeerd voor het toetsen van gegevensverstrekking aan externe partijen, dat consequent wordt toegepast in de gehele organisatie. b. De organisatie heeft het kader met daarin zowel het toetsingsproces als de besluitvorming daaromtrent gedocumenteerd. c. Relevante medewerkers (zoals inkoop, juridische afdeling, onderzoekers) zijn goed geïnformeerd over het belang van voorafgaande toetsing van de gegevensverstrekking aan externe partijen en zijn actief betrokken bij deze processen. d. Medewerkers weten wie ze kunnen benaderen om te toetsen of een eenmalige gegevensverstrekking in overeenstemming is met de wet- en regelgeving.

Wat	Beschrijving
VWN4 - beheerst	a. De organisatie voert periodiek systematische controles uit om ervoor te zorgen dat de gegevensverstrekking aan externe partijen steeds voldoet aan de meest recente wet- en regelgeving. b. De toetsingsprocedures worden periodiek geëvalueerd en indien nodig aangepast. c. Training en bewustmaking over gegevensverstrekking aan externe partijen zijn geïntegreerd in de reguliere bedrijfsprocessen en -procedures. d. Er is een gemakkelijk vindbaar overzicht van alle gegevensverstrekkingen aan externe partijen beschikbaar, bijvoorbeeld via een specifieke interne tool of systeem.
VWN5 - geoptimaliseerd	a. De organisatie is in staat om snel te reageren op wijzigingen in wet- en regelgeving die de gegevensverstrekking aan externe partijen kunnen beïnvloeden, en kan procedures en praktijken dienovereenkomstig aanpassen.
AVG-UAVG	AVG 5 AVG 6
ISO 27701:2019	7.5 8.5
VNG 3.0	5.2
Norea PCF	• TPD01 • UKI01

SW.03 - Doorgifte buiten EER

Wat	Beschrijving
Domein	Samenwerking
Categorie	Doorgifte buiten de EER
Beschrijving risico	Het niet toetsen en waarborgen van een passend beschermingsniveau bij doorgifte van persoonsgegevens naar buiten de EER kan leiden tot ongeautoriseerde toegang, onrechtmatige verwerking en onvoldoende bescherming van persoonsgegevens. Dit kan ertoe leiden dat rechten en vrijheden van betrokkenen onvoldoende zijn beschermd en rechtsbescherming van betrokkenen buiten de EER ontbreekt waardoor betrokkenen niet alleen controle over hun persoonsgegevens zijn verloren maar ook hun rechten onder de AVG niet naar behoren kunnen uitoefenen. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door onrechtmatige verwerking en/of onvoldoende bescherming van persoonsgegevens. Voor de organisatie: • onrechtmatige verwerking. • imago- of reputatieschade. • dwangmaatregelen of boetes opgelegd door de toezichthouder. • schadeclaims van gedupeerden. • hogere kosten door naderhand (reparatie-) maatregelen te moeten nemen.
Beheerdoelstelling	Doorgifte van persoonsgegevens buiten de EER vindt uitsluitend plaats wanneer een passend beschermingsniveau is gewaarborgd.
Toelichting	Voordat de organisatie persoonsgegevens doorgeeft aan verwerkers of ontvangers in derde landen, beoordeelt de organisatie of de Europese Unie voor dit land een adequaatheidsbesluit heeft genomen. Zo niet, dan is er een procedure vastgesteld om te bepalen of doorgifte buiten de EER voldoet aan een passend beschermingsniveau. Als een adequaatheidsbesluit ontbreekt, moet 'passend beschermingsniveau' aangetoond worden d.m.v. een DTIA (Data Transfer Impact Assessment). Hierbij kan gebruik gemaakt worden van het afwegingskader van de Taskforce Beyond Privacy Shield.
Toetsing	O&P
VWN1 - ad hoc	a. Binnen de organisatie is er onvoldoende bekendheid over de procedures die moeten worden gevolgd bij het overdragen van gegevens buiten de EER. b. De organisatie heeft geen (duidelijk) inzicht in de landen waaraan persoonsgegevens worden doorgegeven. c. Periodieke toetsing van de naleving van wet- en regelgeving met betrekking tot de doorgifte van persoonsgegevens aan derde landen (buiten de EER) ontbreekt.
VWN2 - herhaalbaar	a. De organisatie voert voorafgaand aan een voorgenomen doorgifte naar een derde land buiten de EER een toetsing uit of bij doorgifte de verwerking aan een passend beschermingsniveau voldoet, maar het proces is niet (volledig) gedocumenteerd en de kennis en expertise is slechts bij een beperkt aantal individuen binnen organisatie aanwezig. b. Er is geen gestandaardiseerde procedure voor het documenteren van landen waaraan persoonsgegevens worden doorgegeven wat het risico op inconsistenties en fouten verhoogt.
VWN3 - bepaald	a. De organisatie voert voorafgaand aan een voorgenomen doorgifte buiten de EER een systematisch toetsing uit om te beoordelen of bij doorgifte de verwerking aan een passend beschermingsniveau voldoet. b. Er is een duidelijk en consistent proces voor het documenteren van landen waaraan persoonsgegevens worden doorgegeven.

Wat	Beschrijving
	c. Periodiek wordt getoetst of de doorgifte naar derde landen buiten de EER (nog) aan de wet- en regelgeving voldoet. Het proces voor deze toetsing is gedocumenteerd en bekend bij de medewerkers.
VWN4 - beheerst	a. De organisatie evalueert periodiek de doorgiftes buiten de EER en past indien nodig de (toets-)processen aan. b. De periodieke evaluaties worden ondersteund door bewustwordingscampagnes en/of training om de kennis en het bewustzijn over doorgiftes buiten de EER binnen de organisatie te verhogen.
VWN5 - geoptimaliseerd	a. De organisatie heeft een tool geïmplementeerd om inzicht te krijgen in gegevensverstrekkingen waaronder doorgiftes naar derde landen, wat ook het proces van het monitoren en periodiek evalueren van de gegevensverstrekkingen vergemakkelijkt. b. De organisatie is in staat om te reageren op veranderingen in de omstandigheden of wet- en regelgeving over doorgifte buiten de EER.
AVG-UAVG	AVG 27 AVG 44 AVG 45 AVG 46 AVG 47 AVG 48 AVG 49
ISO 27701:2019	6.3.1.1 7.5 8.5
VNG 3.0	5.2
Norea PCF	• PPO05 • DTR01 • DTR02

Gegevensbescherming

GB.01 - Datalekken behandelen

Wat	Beschrijving
Domein	Gegevensbescherming
Categorie	Datalekken detectie, classificatie en afhandeling
Beschrijving risico	Het ontbreken van een gestructureerd proces voor de detectie en afhandeling van datalekken kan leiden tot vertragingen, inefficiëntie en onvoldoende respons. Het gebrek aan duidelijke procedures kan resulteren in onvolledige of inadequaat beheerde datalekken. Dit kan de impact van het datalek vergroten, het herstel bemoeilijken en de schade voor betrokkenen en de organisatie vergroten. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door het niet tijdig detecteren of afhandelen van datalekken. Voor de organisatie: • imago- of reputatieschade. • gebrek aan vertouwen. • dwangmaatregelen of boetes opgelegd door de toezichthouder. • schadeclaims van gedupeerden. • hogere kosten door naderhand (reparatie-) maatregelen te moeten nemen.
Beheerdoelstelling	De organisatie heeft een proces vastgesteld en gedocumenteerd voor de detectie, classificatie en be-/afhandeling van datalekken.
Toelichting	Het proces om datalekken af te handelen kan ook onderdeel zijn van het bestaande incident managementproces, zo niet dan zijn beide processen op elkaar afgestemd. Dit brengt een administratie/registratie met zich mee ten aanzien van (mogelijke / gemelddatalekken. Het datalekkenregsiter bevat ten minste: • een omschrijving van het datalek; • wanneer het datalek heeft plaats gevonden; • beschrijving wat er met de persoonsgegevens is gebeurd; • beschrijving van welke groep(en) personen er gegevens zijn gelekt; • beschrijving van het type gegevens; • de mogelijke gevolgen van het datalek; • de maatregelen die zijn genomen om de schade te beperken en om herhaling te voorkomen.
Toetsing	O&P
VWN1 - ad hoc	a. Er ontbreekt een (centraal) meldpunt voor privacyincidenten dat toegankelijk is voor alle medewerkers, onderwijsdeelnemers en overige betrokkenen. b. Er is geen gestructureerd proces voor het detecteren, classificeren en afhandelen van datalekken. c. Er is niet duidelijk wanneer een (beveiligings)incident een datalek is. d. Incidenten worden afgehandeld op ad hoc basis, en worden niet geëvalueerd. e. Er is geen datalekkenregister.
VWN2 - herhaalbaar	a. Er is geen makkelijk vindbaar meldpunt voor privacyincidenten voor alle medewerkers, onderwijsdeelnemers en overige betrokkenen, en/of het is niet gemakkelijk toegankelijk. b. Er is een informeel proces voor het detecteren, classificeren en afhandelen van datalekken, maar medewerkers zijn onvoldoende opgeleid om adequaat te reageren op incidenten waarbij persoonsgegevens zijn betrokken. c. Classificatie van incidenten waarbij persoonsgegevens zijn betrokken op impact/ risico voor betrokkenen is afhankelijk van de individuele medewerker die de classificatie uitvoert. d. Evaluatie van incidenten waarbij persoonsgegevens zijn betrokken wordt ad hoc uitgevoerd.

Wat	Beschrijving
	e. Het datalekkenregister wordt ad hoc ingevuld.
VWN3 - bepaald	a. Er is een makkelijk vindbaar en gemakkelijk toegankelijk meldpunt voor privacyincidenten. b. Er is een gedetailleerd proces gedefinieerd en gedocumenteerd voor het detecteren, classificeren en afhandelen van datalekken. Het proces omvat ten minste: • een beschrijving van rollen, verantwoordelijkheden en contactpersonen, • detectie en identificatie van een datalek, • een risicobeoordeling c.q. afwegingskader waar het al dan niet melden van een datalek onderdeel van is • respons- en escalatie, • beheersing, • herstel, • evaluatie c. Incidenten worden systematisch geëvalueerd om verbeteringen te identificeren. d. De resultaten van de evaluaties worden met het management gedeeld. e. Er is een datalekkenregister dat regelmatig wordt bijgewerkt. Het register bevat alle (gemelde) datalekken.
VWN4 - beheerst	a. Het proces voor het detecteren, classificeren en afhandelen van datalekken wordt periodiek geëvalueerd om de effectiviteit ervan te waarborgen en indien nodig aangepast. b. De vindbaarheid van het privacy meldpunt wordt periodiek geëvalueerd. c. Het datalekkenregister wordt regelmatig geëvalueerd.
VWN5 - geoptimaliseerd	a. Het proces voor het detecteren, classificeren en afhandelen van datalekken is volledig geïntegreerd en er is een proactieve aanpak om mogelijke toekomstige incidenten te identificeren en te voorkomen. b. Deze resultaten van de evaluatie van datalekken worden gedeeld met het management en indien van toepassing binnen de gehele organisatie. c. De organisatie gebruikt de informatie uit het register proactief om toekomstige datalekken te voorkomen en de algehele privacy te verbeteren.
AVG-UAVG	VG 4 sub 12, AVG 33 AVG 34
ISO 27701:2019	6.3.1.1
VNG 3.0	6.5
Norea PCF	• PBI01 • PBI03 • PBI04 • PBI05 • PBI06 • PBI07 • PBI08 • PBI09

GB.02 - Datalekken communiceren

Wat	Beschrijving
Domein	Gegevensbescherming
Categorie	Melding van datalekken aan AP en betrokkenen
Beschrijving risico	Het niet tijdig mededelen van inbreuk op de persoonsgegevens met hoog risico voor de rechten en vrijheden van betrokkenen leidt ertoe dat betrokkenen niet in staat worden gesteld om maatregelen te treffen om de negatieve consequenties op de persoonlijke levenssfeer te beperken. Het niet tijdig en volledig melden van datalekken aan de AP kan resulteren in schending van de verplichtingen volgend uit artikel 33 van de AVG. Het ontbreken van duidelijke verantwoordelijkheden en tijdslijnen kan het proces vertragen en de impact onnodig vergroten. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door het niet tijdig mededelen van inbreuk op de persoonsgegevens met hoog risico voor betrokkenen. Voor de organisatie: • imago- of reputatieschade. • gebrek aan vertrouwen. • dwangmaatregelen of boetes opgelegd door de toezichthouder. • schadeclaims van gedupeerden.
Beheerdoelstelling	De organisatie heeft een gestructureerd proces ingericht en gedocumenteerd voor het tijdig en volledig registreren en (eventueel) melden van datalekken aan de relevante partijen, inclusief de AP en de betrokkenen.
Toelichting	Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, en er een risico is voor betrokkene, meldt de verwerkingsverantwoordelijke dit aan de Autoriteit Persoonsgegevens. Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, deelt de verwerkingsverantwoordelijke de inbreuk in verband met persoonsgegevens mee aan de betrokkene(n). In dit toetsingskader noemen we beiden "melden". Aanbevolen wordt om een woordvoerder beschikbaar te hebben die in voorkomende gevallen gedupeerde betrokkenen en/of de media te woord kan staan. Met woordvoerder wordt niet de functie van woordvoerder bedoeld, maar de rol.
Toetsing	O
VWN1 - ad hoc	a. Er is geen proces voor melden van datalekken aan de AP en betrokkenen. b. Er is geen duidelijkheid over wie verantwoordelijk is voor het melden van een datalek aan de AP en betrokkenen. c. Er zijn geen vastgestelde tijdslijnen voor het melden van een datalek aan de AP en betrokkenen. d. Er is geen woordvoerder voor de communicatie over (mogelijke) datalekken met betrokkenen en/of media.
VWN2 - herhaalbaar	a. Er bestaat een Informeel proces voor het melden van datalekken aan de AP en betrokkenen, maar de implementatie en naleving zijn inconsistent. b. Verantwoordelijkheden voor het afhandelen en communiceren van datalekken zijn gedefinieerd, maar zijn niet altijd duidelijk voor alle betrokken partijen. c. De tijdslijnen waarbinnen datalekken worden gemeld zijn wisselend en er is geen vastgesteld proces voor het documenteren van de afhandeling van een datalek. Classificatie van de ernst (risicobeoordeling) van een datalek is afhankelijk van de betrokkenen.

Wat	Beschrijving
VWN3 - bepaald	a. Er is een gedetailleerd en gedocumenteerd proces voor het melden van datalekken aan de AP en betrokkenen, met daarin ten minste: • communicatierichtlijnen voor melding aan AP en betrokkenen, • duidelijk gedefinieerde verantwoordelijkheden, • documentatievereisten en tijdslijnen. b. Er is een crisiscommunicatieplan voor datalekken met hoge impact. c. Het proces wordt consistent nageleefd.
VWN4 - beheerst	a. Het proces voor het melden van datalekken aan de AP en betrokkenen is volledig geïntegreerd in de organisatie, met consistente uitvoering en naleving. b. Het proces voor het melden van datalekken aan de AP en betrokkenen wordt periodiek geëvalueerd en, indien nodig, aangepast. c. Het crisiscommunicatieplan voor datalekken met hoge impact wordt periodiek geoefend, en indien nodig, herzien.
VWN5 - geoptimaliseerd	a. Het proces voor het melden van datalekken aan de AP en betrokkenen is een standaard onderdeel van de bedrijfsvoering, wordt systematisch nageleefd en continu geëvalueerd en verbeterd. b. Het management wordt systematisch geïnformeerd over alle datalekken en genomen maatregelen. c. Er bestaat een hiërarchie (escalatieregels) voor escalatie naar de juiste managementniveaus.
AVG-UAVG	AVG 4 sub 12, AVG 33 AVG 34
ISO 27701:2019	6.13.1.1
VNG 3.0	6.5
Norea PCF	• PBI01 • PBI03 • PBI04 • PBI05 • PBI06 • PBI07 • PBI08 • PBI09

GB.03 – Informatiebeveiliging

Wat	Beschrijving
Domein	Gegevensbescherming
Categorie	Informatieveiligheid
Beschrijving risico	Het ontbreken van passende, organisatorische en technische maatregelen om, conform artikel 32 van de AVG, een op het risico afgestemd beveiligingsniveau te waarborgen, kan leiden tot het ongewenst openbaar worden, manipulatie, misbruik en niet beschikbaar zijn van gegevens. Dit kan leiden tot: Voor betrokkenen: • risico's voor de rechten en vrijheden van personen door het ongewenst openbaar worden, manipulatie of niet beschikbaar zijn van gegevens. Voor de organisatie: • datalekken. • imago- of reputatieschade. • gebrek aan vertrouwen. • dwangmaatregelen of boetes opgelegd door de toezichthouder. • schadeclaims van gedupeerden. • hogere kosten door naderhand (reparatie-) maatregelen te moeten nemen.
Beheerdoelstelling	Adequate informatiebeveiliging om persoonsgegevens te beschermen. De relevante IB-maatregelen die hierbij passen: • GO.02 - Beleid • GO.05 - Onafhankelijke toetsing • OR.01 - Eigenaarschap, rollen, verantwoording en verantwoordelijkheid • RM.02 - Risicobeoordeling • DM.02 - Classificatie • DM.03 - Beveiligingseisen voor gegevensbeheer • DM.05 - Uitwisseling van (gevoelige) gegevens • ID.01 - Toegangsrechten • ID.02 - Administratie van toegangsrechten • ID.05 - Periodieke beoordeling van toegangsrechten • SM.01 - Security baselines • SM.02 - Authenticatie-mechanismes • SM.04 - Logging
Toelichting	De IB-maatregelen voor het SURFaudit Toetsingskader Privacy overlappen (grotendeels) met de maatregelen uit het SURFaudit Toetsingskader Informatiebeveiliging. Omdat iedere organisatie periodiek een audit (of self assessment) uitvoert met het SURFaudit Toetsingskader informatiebeveiliging kan worden volstaan om hier het resultaat van deze audit op te nemen. Hiermee wordt voorkomen dat beveiligingsmaatregelen meermaals getoetst moeten worden. Het cijfer mag naar beneden worden afgerond als het na de komma 0, 1, 2, 3 of 4 is, en anders kan het naar boven afgerond worden. Voor interne rapportage over privacy raden we aan om vooral te kijken naar de voor GB.03 vastgestelde, relevante IB-maatregelen. Artikel 32 lid 1 stelt dat de beveiliging onder meer het volgende moet omvatten: • de pseudonimisering en versleuteling van persoonsgegevens; • het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid de veerkracht van de verwerkingssystemen en diensten te garanderen; • het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen; • een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Verantwoording

VW.01 – Rapportage

Wat	Beschrijving
Domein	Verantwoording
Categorie	Rapportage
Beschrijving risico	Door transparant en regelmatig aan in- en externe stakeholders te rapporteren over hoe de organisatie omgaat met de bescherming van persoonsgegevens en de naleving van de AVG kan zij daarmee aantonen dat zij zorgvuldig omgaat met de rechten en vrijheden van personen/betrokkenen. Het niet of niet periodiek rapporteren aan interne en externe stakeholders kan leiden tot onduidelijkheid, misverstanden en wantrouwen over de mate waarin de organisatie conform de AVG uitvoering geeft aan de rechten en vrijheden van personen/betrokkenen. Dit kan leiden tot: Voor de organisatie: • imago- of reputatieschade. • gebrek aan vertrouwen. • dwangmaatregelen of boetes opgelegd door de toezichthouder.
Beheerdoelstelling	De organisatie houdt periodiek interne en externe stakeholders op de hoogte over de naleving van de AVG.
Toelichting	Geadviseerd wordt om in het periodieke privacy verslag voor interne stakeholders ten minste de volgende onderwerpen op te nemen: • globaal overzicht verwerkingsregister. • uitgevoerde DPIA's. • verslag over datalekken. • verzoeken rechten van betrokkenen. • resultaten van het SURFaudit Toetsingskader Privacy benchmark. • verbeterplan. Voor verantwoording aan externe stakeholders kan worden gedacht aan: • informatie voor onderwijsdeelnemers. • een alinea/paragraaf in het algemene jaarverslag van de organisatie, gebaseerd op het uitgebreidere interne privacy verslag. N.B. Dit privacyverslag betreft niet het verslag dat de FG vanuit zijn/haar toezichthoudersrol opstelt
Toetsing	O&P
VWN1 - ad hoc	a. Er wordt geen periodiek verslag gemaakt om interne (inclusief het bestuur) en externe stakeholders te informeren over de omgang met en bescherming van persoonsgegevens binnen de organisatie. b. Informatie van afdelingen over de omgang met en bescherming van persoonsgegevens binnen hun afdeling of hun processen wordt niet periodiek (centraal) verzameld. Hierdoor kan er geen organisatiebreed inzicht worden verschaft over de naleving van de AVG.
VWN2 - herhaalbaar	c. Er wordt periodiek een verslag opgesteld voor zowel interne (inclusief het bestuur) als externe stakeholders over de omgang met en bescherming van persoonsgegevens binnen de organisatie, maar dit proces is niet gedocumenteerd en de FG wordt niet consequent betrokken. d. Informatie van afdelingen over de omgang met en bescherming van persoonsgegevens wordt periodiek (centraal) verzameld, maar dit proces is niet volledig gedocumenteerd en gebeurt niet op een structurele en georganiseerde manier.
VWN3 - bepaald	e. Er wordt een gestructureerd en gedocumenteerd proces gevolgd voor het opstellen van een periodiek verslag waarin zowel interne (inclusief het bestuur) als externe stakeholders

Wat	Beschrijving
	worden geïnformeerd over de omgang met en bescherming van persoonsgegevens binnen de organisatie. De FG wordt betrokken en geraadpleegd bij het opstellen van dit verslag. f. Informatie van afdelingen over de omgang met en bescherming van persoonsgegevens wordt periodiek centraal verzameld op een gestructureerde manier, waardoor de bestuursorganen organisatiebreed inzicht kunnen krijgen in de naleving van de AVG. g. Dit proces omvat het periodiek opstellen van een organisatieverslag waarin verschillende aspecten worden behandeld, bijvoorbeeld het globale overzicht van het verwerkingsregister, uitgevoerde DPIA's, verslag over datalekken, verzoeken rechten van betrokkenen, resultaten van de privacy benchmark en verbeterplannen. h. De verantwoordelijkheden voor het opstellen en verspreiden van dit verslag zijn duidelijk aantoonbaar toegewezen.
VWN4 - beheerst	i. De inhoudelijke elementen van de rapportage en het rapportageproces worden periodiek geëvalueerd en indien nodig aangepast. j. Op basis van rapportage worden verbeterplannen opgesteld en wordt gerapporteerd over de uitvoering hiervan.
VWN5 - geoptimaliseerd	k. Er is een volledig geïntegreerd proces voor het opstellen van periodieke rapportage en het centraal verzamelen van informatie van afdelingen. Dit proces wordt systematisch nageleefd en continu geëvalueerd en verbeterd. l. Naast de reguliere periodieke rapportage, worden interne en externe stakeholders ook ad-hoc geïnformeerd over belangrijke in- en externe ontwikkelingen met betrekking tot de bescherming van persoonsgegevens. m. Er wordt gebruik gemaakt van tools en methodes om informatie op een toegankelijke en begrijpelijke manier te presenteren,bijvoorbeeld via animaties. n. Er vindt periodiek uitwisseling plaats met andere organisatie om ervaringen, best practices en leerpunten te delen op het gebied van AVG-naleving en transparantie. verantwoording en rapportage.
AVG-UAVG	AVG5 lid 2 AVG 39
ISO 27701:2019	-
VNG 3.0	7.3
Norea PCF	

Bijlage – Uitleg volwassenheidsniveaus

In het SURFaudit toetsingskader privacy is ervoor gekozen om aan te sluiten bij de vijf volwassenheidsniveaus van het 'Privacy maturity model' van de IAPP. Deze niveaus van de IAPP zijn weer afgeleid van de GAPP's (Generally Accepted Privacy Principles) en het CMM (Capability Maturity Model). Ook in andere landen wordt het model toegepast. Zie bijvoorbeeld een onderzoek naar de volwassenheid van het beschermen van persoonsgegevens van Zweedse gemeenten in 2019: https://gupea.ub.gu.se/handle/2077/61846.

Matrix volwassenheid

1	Ad hoc	• Geen of onduidelijke privacyrollen en -verantwoordelijkheden • Geen of nauwelijks beheersmaatregelen aanwezig • Reactief en sturing n.a.v. incidenten • Grote afhankelijkheid van één of enkele privacyfunctionarissen • Onbewust onbekwaam
2	Herhaalbaar	• Privacyrollen en -verantwoordelijkheden toegewezen • Beheersmaatregelen zijn aanwezig, maar worden op informele wijze uitgevoerd • Standaarden en formats aanwezig: juist en in duidelijke taal • Bewust onbekwaam
3	Bepaald	• (Privacy)medewerkers tonen eigenaarschap, d.w.z. dat de rollen en • verantwoordelijkheden actief worden opgepakt • Beheersmaatregelen worden consistent en gestructureerd uitgevoerd en zijn gedocumenteerd • Er wordt aantoonbaar aan verplichtingen voldaan • Verwerkingsverantwoordelijke bestuursorganen nemen beslissingen mede op grond van risicoanalyses zoals een DPIA. • Er is een duidelijke samenhang met informatiebeveiliging • Bewust bekwaam
4	Beheerst	• De effectiviteit van beheersmaatregelen wordt periodiek geëvalueerd in een PDCA-cyclus • Er wordt proactief geïnformeerd door de proceseigenaar over de realisering van de geconstateerde benodigde verbeteringen in een PDCA-cyclus • In een jaarlijkse evaluatie blijkt een correcte PDCA-cyclus • Bewust bekwaam
5	Geoptimaliseerd	• Toekomstgericht • Proactieve houding van het college en het bestuur • Het verantwoordelijk management verzoekt aan de FG om hun verantwoording van een oordeel te voorzien. • Privacy wordt gezien als een vanzelfsprekendheid • Er wordt continue gezocht naar verbetering, zoals in de vorm van (interne of externe) tooling • Privacy wordt gezien als een kans of unique selling point (USP) • Er wordt verbinding gezocht met andere concerndisciplines • Kennis en ervaringen worden actief gedeeld met andere instellingen en SURF en andere relevante organisaties waardoor best practices in de HO-sector ontstaan • Onbewust bekwaam

Overwegingen volwassenheidsniveaus

De volgende overwegingen zijn van belang bij deze privacyvolwassenheidsniveaus:

- De proceseigenaren zijn verantwoordelijk voor de uitvoering van de statements en beheersmaatregelen en het streefniveau op een bepaald domein kan worden bepaald door het management. Het college of een door hen gemandateerde kan het streefniveau vaststellen.
- Vanaf niveau 3 "stapelen" de maatregelen. Dit betekent dat bij niveau 4 ook aan de beheersmaatregelen van niveau 3 voldaan moet zijn. Op niveau 1 zijn er slechts minimale beheersmaatregelen genomen. Niveau 2 fungeert voornamelijk als een tussenstap tussen niveau 1 en 3, om een instelling te helpen duidelijker inzicht te krijgen in mogelijke groeistappen.
- Het volwassenheidsniveau wordt alleen behaald als aan alle maatregelen van dat niveau en de maatregelen van de lagere niveaus wordt voldaan, met uitzondering van de maatregelen op niveaus 1 en 2.
- Niveau 3 wordt beschouwd als het sectorale minimum ambitieniveau voor alle statements. Hiermee is niet gezegd dat de instelling volledig AVG-compliant is als voor alle statements niveau 3 is bereikt, omdat de maatregelen binnen een bepaald volwassenheidsniveau niet uitputtend zijn.
- Niveau 5 is het hoogst haalbare volwassenheidsniveau. Sommige zaken spelen ook pas een rol als de basis goed op orde is, zoals het gebruik van tooling ter ondersteuning van bepaalde processen. Verder kunnen onderdelen van dit niveau dienen ter inspiratie in de vorige niveaus. Aantoonbaarheid van niveau 5 is soms uitdagend, maar kan bijvoorbeeld ook gezocht worden in verslagen van bijeenkomsten of rapportages.
- Denk bij andere concerndisciplines (niveau 5) bijvoorbeeld aan informatiebeveiliging, informatiebeheer en risicomanagement.
- Beheersmaatregelen of delen van volwassenheidsniveaus kunnen een rol spelen bij andere lagere niveaus. Zo wordt bij niveau 5 een proactieve houding van het bestuur gevraagd. Het is natuurlijk mogelijk dat het bestuur al een proactieve houding heeft, terwijl de instelling ‘slechts’ bij niveau 2 is.

Bijlage – terminologie

In het toetsingskader zijn beheerdoelstellingen opgenomen die een norm stellen. In de volwassenheidsniveaus zijn vervolgens de maatregelen opgenomen waarmee je aan de beheerdoelstelling kunt voldoen. Voor de juiste interpretatie lichten we hieronder de terminologie toe.

- **Aantoonbaar**
  Een maatregel kan onder andere worden aangetoond met documenten, verslagen, screenshots, tickets uit een ticketsysteem, et cetera.
- **Aantonen dat een evaluatie is uitgevoerd**
  Dit kan worden aangetoond met verslagen van deze evaluaties en eventuele acties die daaruit voortvloeien.
- **Beleid, wijzigingen, et cetera actief communiceren**
  Bijvoorbeeld met e-mails, aankondigingen op het intranet, trainingen, vergaderingen, et cetera.
- Evalueren (meestal volwassenheidsniveau 4)
  Voor evaluatie zijn de volgend aspecten van belang: actualiteit, effectiviteit, voldoen aan wet- en regelgeving, voldoen aan best practices.
- **Procedure**
  Een procedure is een vastgelegde manier van handelingen uitvoeren. Het gaat om een specifiek omschreven volgorde van stappen die genomen moeten worden in een proces.
- **Proces**
  Een proces is een samenhangend geheel van activiteiten, mensen en middelen, waarmee één of meer producten of diensten worden voortgebracht. Een proces kunnen we veelal uiteenrafelen in activiteiten en een activiteit kan weer bestaan uit meerdere handelingen (die in een procedure zijn vastgelegd). Meerdere processen die op een logische wijze op elkaar volgen, noemen we een procesketen.
  Voorbeelden van processen binnen de sector onderwijs en onderzoek zijn: het studenten inschrijfproces (ATI-proces), het toetsingsproces, het onderwijsproces, het onderzoeksproces, het HR-proces, et cetera. Een proces kan over verschillende afdelingen en soms zelfs verschillende organisaties heen lopen. Een proces kan meerdere gegevensverwerkingen omvatten.
- **Procesbeschrijving**
  Een procesbeschrijving beschrijft hoe een proces verloopt en wie ervoor verantwoordelijk is. Een procesbeschrijving bevat minimaal een titel, een proceseigenaar, en een (korte) beschrijving van het proces.
- **Makkelijk vindbaar, eenvoudig toegankelijk**
  Als iets alleen voor intern gebruik is: bijvoorbeeld via het intranet en gemakkelijk op te zoeken.
  Als iets ook voor externen bedoeld is: op de publiek website en gemakkelijk op te zoeken.
- **Vastgesteld**
  Bijvoorbeeld beleid: een door een CvB-lid ondertekend document, een verslag van een CvB-vergadering met daarin het besluit of een besluitenlijst kan dienen als bewijslast. Bijvoorbeeld een DPIA: een door een gemandateerde functionaris (bijvoorbeeld een proceseigenaar) schriftelijke goedkeuring. Dit kan ook een verslag zijn waarin de goedkeuring is opgetekend.