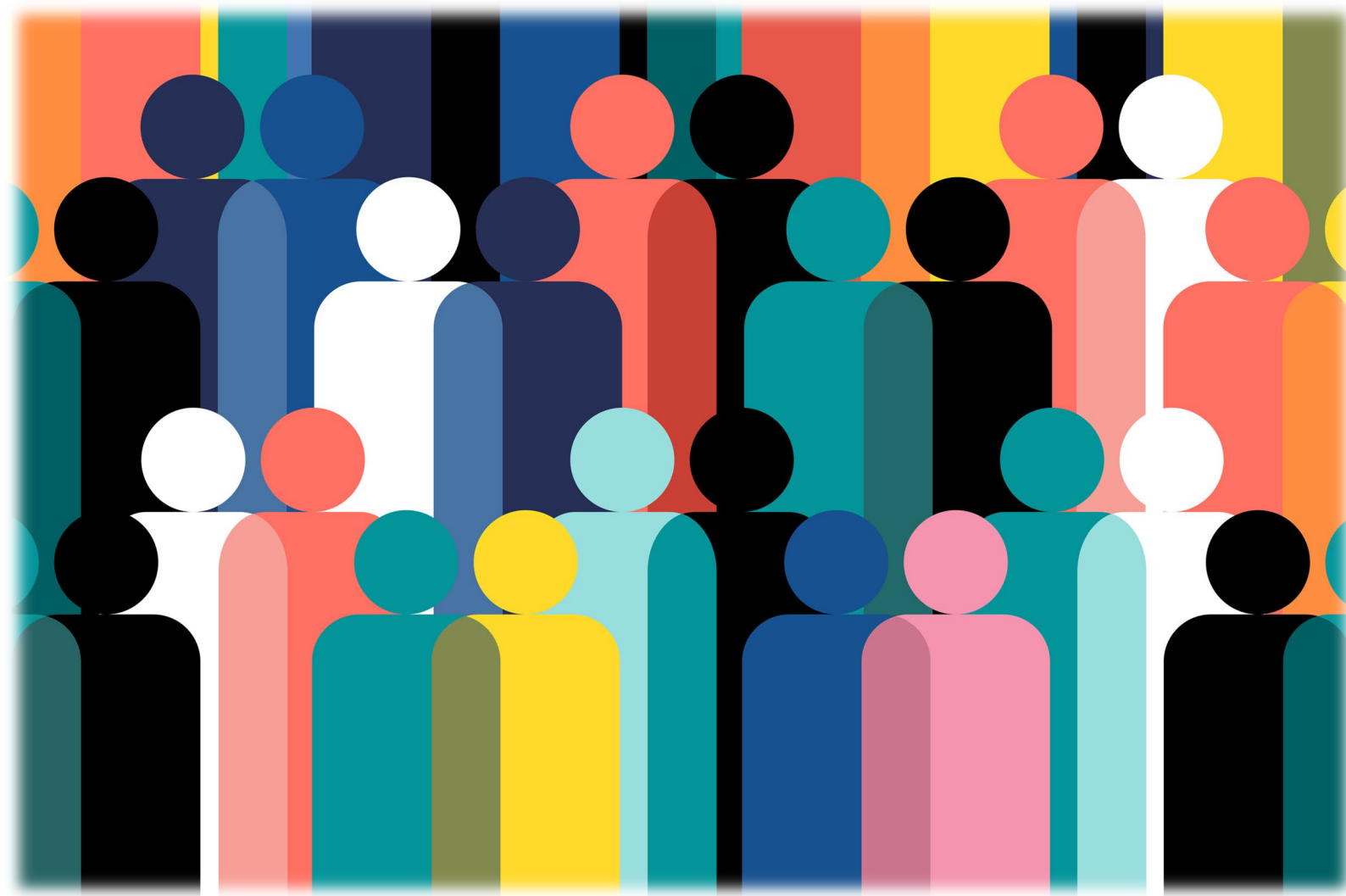




Samen aanjagen van vernieuwing

SURF Toetsingskader Privacy



Inhoudsopgave

Colofon	3
Inleiding	4
De beheerdoelstellingen in het domein beveiliging	4
Jaarlijkse benchmark via SURFaudit	4
Domein Beleid	5
BL.01 - Privacybeleid	5
BL.02 - Rollen, taken en verantwoordelijkheden	8
BL.03 – Risico's	11
Processen	14
PR.01 - Operationele processen	14
PR.02 - Verwerkingsregister inrichten	17
PR.03 - Verwerkingsregister actualiseren	21
PR.04 – Risico-inschatting (pre-DPIA)	24
PR.05 - DPIA's	27
PR.06 - Privacy by Design	31
PR.07 - Bewaren en vernietigen	35
Organisatorische inbedding	38
OI.01 – FG	38
OI.02 – Privacyteam	42
OI.03 – Betrokkenheid	45
OI.04 – Bewustwording	48
Rechten van betrokkenen	51
RB.01 - Rechten van betrokkenen	51
RB.02 – Informatieplicht	55
RB.03 – Toestemming	59
RB.04 - Geautomatiseerde besluitvorming	63
Samenwerking	66
SW.01 - Externe AVG-rollen	66
SW.02 - Eenmalige verstrekkingen	70
SW.03 - Doorgifte buiten EER	73
Gegevensbescherming	76
GB.01 - Datalekken behandelen	76
GB.02 - Datalekken communiceren	79
GB.03 – Informatiebeveiliging	82
Verantwoording	86
VW.01 – Rapportage	86
Bijlage – Uitleg volwassenheidsniveaus	89
Overwegingen volwassenheidsniveaus	91
Bijlage – terminologie	92

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 Zijdam	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, Helma de Boer.

Naam document

SURF Toetsingskader Privacy

Versienummer en -datum

Versie 3.2, 11 november 2025 (samenvoeging volwassenheidsniveaus en bewijsmateriaal)

Beheer

Het beheer van dit document berust vanaf mei 2025 bij het [Privacy Expertise Centrum](#) van SURF. Voor inhoudelijke 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

Het Toetsingskader Privacy is afgeleid van het Borgingsproduct AVG van de Informatiebeveiligingsdienst voor gemeenten (IBD) / Vereniging van Nederlandse Gemeenten (VNG). Tenzij anders vermeld, is dit werk verstrekt onder een Creative Commons Naamsvermelding-Niet Commercieel-Gelijk Delen 4.0 Internationaal licentie. Dit houdt in dat het materiaal gebruikt en gedeeld mag worden onder de volgende voorwaarden: Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties. Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden: SURF, IBD en VNG worden als bron vermeld. Het document en de inhoud mogen commercieel niet geëxploiteerd worden. Publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door SURF. Iedere kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Wanneer je dit document gebruikt, hanteer dan de volgende methode van naamsvermelding: "Vereniging van Nederlandse Gemeenten / Informatiebeveiligingsdienst voor gemeenten", licentie onder: CC BY-NC-SA 4.0.

Bezoek <https://creativecommons.org/licenses/by-nc-sa/4.0> voor meer informatie over de licentie.



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 (zie de bijlage voor uitleg over die niveaus). 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 ambitieniveau 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 beheerdoelstelling Informatiebeveiliging GB.03 (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	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • imago- of reputatieschade • gebrek aan vertrouwen • dwangmaatregelen of boetes opgelegd door de toezichthouder
Beheerdoelstelling	Er is privacybeleid vastgesteld voor de gehele organisatie.
Toelichting	<p>De organisatie dient aantoonbaar uitvoering te geven aan de privacybeginselen op grond van art. 5 lid 2 AVG (verantwoordingsplicht).</p> <p>Met formeel vastgesteld verstaan we dat het College van Bestuur (of Raad van Bestuur) het privacybeleid heeft vastgesteld.</p> <p>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.</p> <p>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.</p>
Toetsing	O&P
AVG-UAVG	AVG 24 lid 2
ISO 27701:2019	6.2
VNG 3.0	1.2
Norea PCF	<ul style="list-style-type: none"> • PP001 • PP002 • PP003 • PP004 <ul style="list-style-type: none"> • DMI02 • ULIO2 • RRE054 • RRE055

BL.01 – Bewijsmateriaal Privacybeleid per volwassenheidsniveau

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Het privacybeleid bestaat in concept of er is geen beleid opgesteld.	•
VWN2 - herhaalbaar	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	Het privacybeleid is actueel en beschrijft hoe de organisatie uitvoering geeft aan de privacybeginselen die in art 5 lid 1 AVG zijn vastgelegd.	<ul style="list-style-type: none"> • Een actuele versie van het (gepubliceerde) privacybeleid dat expliciet de privacybeginselen van de AVG adresseert en hoe de organisatie deze beginselen in de praktijk brengt. • Versiebeheer: een wijzigingslogboek of revisiegeschiedenis van het privacybeleid om aan te tonen dat het regelmatig wordt geactualiseerd.
	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.	<ul style="list-style-type: none"> • Specifieke secties uit het privacybeleid waarin deze verplichtingen worden beschreven. • Documentatie of processen/procesbeschrijvingen die aantonen hoe de organisatie deze verplichtingen in de praktijk invulling geeft en naleeft. Denk aan een korte privacycheck of -toets per verwerking. Inspiratie: template <<...>>
	Het privacybeleid is formeel door het hoogste management vastgesteld en organisatiebreed bekend, makkelijk vindbaar en makkelijk te begrijpen.	<ul style="list-style-type: none"> • Een document of notulen van een vergadering waaruit blijkt dat het hoogste management het privacybeleid heeft vastgesteld. • Bewijs van hoe het beleid organisatiebreed bekend is gemaakt, zoals interne nieuwsbrieven, e-mails, of intranetberichten. • Screenshots of links naar waar het beleid makkelijk vindbaar is voor alle medewerkers, bijvoorbeeld op het intranet en/of binnen een intern documentbeheersysteem.
	In het beleid is rekening gehouden met (sector-) specifieke wet- en regelgeving, indien van toepassing.	<ul style="list-style-type: none"> • Documentatie die aantoont dat het privacybeleid rekening houdt met specifieke sector- of regionale wet- en regelgeving, indien van toepassing. Denk bijvoorbeeld aan themabeleid m.b.t. Onderwijs & Onderzoek of het toepassen van bewaartermijnen i.r.t. de Wet op het hoger onderwijs en wetenschappelijk onderzoek (Selectielijst).

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
		<ul style="list-style-type: none"> Een overzicht of matrix die de eisen van sectorspecifieke wet- en regelgeving koppelt aan relevante delen van het privacybeleid.
	Wijzigingen in het beleid worden gecommuniceerd.	<ul style="list-style-type: none"> Kopieën van e-mails, nieuwsbriefuitgaven, of berichten op het intranet die de communicatie van wijzigingen in het privacybeleid aantonen.
VWN4 - beheerst	Het privacybeleid wordt periodiek, maar ten minste eenmaal per 36 maanden, geëvalueerd en zo nodig herzien.	<ul style="list-style-type: none">
	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.	<ul style="list-style-type: none">
VWN5 - geoptimaliseerd	Er wordt in het privacybeleid rekening gehouden met toekomstige veranderende wet- en regelgeving, doelstellingen en visie van de organisatie.	<ul style="list-style-type: none">
	Er wordt actief verbinding gezocht met andere (vergelijkbare) organisaties om kennis, ervaring en best practices uit te wisselen.	<ul style="list-style-type: none">

BL.02 - Rollen, taken en verantwoordelijkheden

Wat	Beschrijving
Domein	Beleid
Categorie	Rollen, taken en verantwoordelijkheden
Beschrijving risico	<p>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.</p> <p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>Aanbevolen wordt om een RASCI matrix te hanteren en dit in het privacybeleid vast te leggen. Voor een uitleg van RASCI, zie:</p> <ul style="list-style-type: none"> • Privacy Governance, platform IV-HO <p>Een leidraad hierbij kan ook zijn 3-lines model zijn.</p>
Toetsing	O&P
AVG-UAVG	AVG 24 lid 2 38
ISO 27701:2019	6.3
VNG 3.0	1.3
Norea PCF	<ul style="list-style-type: none"> • PP002 • RRE05 • RMA04

BL.02 – Bewijsmateriaal Rollen, taken en verantwoordelijkheden per volwassenheidsniveau

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Rollen, taken en verantwoordelijkheden met betrekking tot privacy zijn niet duidelijk gedefinieerd en toegewezen binnen de organisatie of zijn niet gedocumenteerd.	•
VWN2 - herhaalbaar	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	Rollen, taken en verantwoordelijkheden met betrekking tot privacy zijn formeel benoemd, belegd en vastgelegd in het privacybeleid en organisatiebreed bekend.	<ul style="list-style-type: none"> • Een kopie van het privacybeleid met specifieke secties die de rollen, taken en verantwoordelijkheden definiëren. • Kopieën van interne communicatie of trainingsmateriaal, zoals e-mails of intranetberichten, die de bekendmaking van deze rollen, taken en verantwoordelijkheden binnen de organisatie aantonen.
	Vastgelegd is dat het hoogste management eindverantwoordelijk is voor privacy binnen de organisatie en dat lijnmanagers verantwoordelijk zijn voor privacy binnen hun managementdomein.	<ul style="list-style-type: none"> • Secties uit het privacybeleid of separate documenten die deze verantwoordelijkheden toewijzen.
	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.	<ul style="list-style-type: none"> • Secties uit het privacybeleid of andere formele documentatie die duidelijk definiëren welke functionaris of rol deze bevoegdheid heeft.
VWN4 - beheerst	Het lijnmanagement legt aantoonbaar verantwoording af over haar taken en verantwoordelijkheden met betrekking tot privacy.	•
	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	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.	•
	Rollen, taken en verantwoordelijkheden met betrekking tot privacy zijn expliciet opgenomen in de functieprofielen van de organisatie, waarmee ze	•

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	een integraal onderdeel zijn van de taken en verantwoordelijkheden van elke medewerker.	
	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.	<ul style="list-style-type: none">•

BL.03 – Risico's

Wat	Beschrijving	
Domein	Beleid	
Categorie	Risico's	
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p>	
Toetsing	O&P	
AVG-UAVG	AVG 32 AVG 24 lid 1	
ISO 27701:2019	5.4	
VNG 3.0	6.1	
Norea PCF	<ul style="list-style-type: none"> • RMA01 • RMA03 • RMA04 • RMA05 • BD02 • ISP01 	<ul style="list-style-type: none"> • ISPO3 • MON01 • MON02 • MON03 • REV01

BL.03 – Bewijsmateriaal Risico's

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Er is geen gedocumenteerd proces binnen de organisatie voor het identificeren, beoordelen en beheren van risico's in de verwerking van persoonsgegevens. De organisatie heeft beperkt inzicht in de risico's bij de verwerking van persoonsgegevens.	<ul style="list-style-type: none">
VWN2 - herhaalbaar	De organisatie heeft een informeel proces geïmplementeerd voor het identificeren, beoordelen en beheren van hoge risico's in de verwerking van persoonsgegevens.	<ul style="list-style-type: none">
VWN3 - bepaald	De organisatie heeft een informeel proces geïmplementeerd voor het identificeren, beoordelen en beheren van hoge risico's in de verwerking van persoonsgegevens.	<ul style="list-style-type: none"> Documentatie van het formele en cyclische proces dat de organisatie hanteert voor het identificeren, beoordelen, en beheren van privacyrisico's in de verwerking van persoonsgegevens i.h.k.v. integraal risicomanagement. Dus organisatiebreed (geen DPIA), zowel risico's voor de organisatie/instelling als in algemene zin voor Betrokkenen. Voorbeelden van (periodieke) risicoanalyses of assessments die met/middels dit proces zijn uitgevoerd, om aan te tonen dat het breed wordt toegepast.
	In het proces is opgenomen dat vastgelegd wordt welke functionaris operationeel verantwoordelijk is voor opvolging van benodigde maatregelen.	<ul style="list-style-type: none"> Specifieke secties van het formele procesdocument of de procedurehandleiding waarin de verantwoordelijkheden van de functionaris worden vastgelegd. Een lijst van aangewezen functionarissen en hun respectievelijke rollen en verantwoordelijkheden in het risicobeheerproces. E.e.a. is vastgelegd in een mandaatregeling of governance-document.
	De organisatie beschikt over een beoordelingskader om risico's te mitigeren.	<ul style="list-style-type: none"> Een kopie van het beoordelingskader dat de organisatie gebruikt om risico's te mitigeren, inclusief criteria, methodologieën en procedures. Er is 'risicomanagement-beleid' waarbinnen een beoordelingskader opgenomen staat? Voorbeelden van hoe dit kader in de praktijk is toegepast bij het beoordelen en mitigeren van specifieke risico's.
	Er is een volledige registratie van hoge risico's.	<ul style="list-style-type: none"> Een actuele lijst of registratie van geïdentificeerde hoge (organisatie) risico's met betrekking tot de verwerking van persoonsgegevens.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	Risicoacceptatie geschiedt op het juiste managementniveau.	<ul style="list-style-type: none"> • Beleidsdocumenten, interne richtlijnen of procedures die aangeven op welk managementniveau risico-acceptatie plaatsvindt, waaruit blijkt dat dit niveau geschikt is gezien de aard en omvang van de risico's. Voorbeelden van risico-acceptatiedocumenten of -beslissingen, inclusief de handtekening of goedkeuring (en datum waarop) van het betreffende managementniveau.
VWN4 - beheerst	Er is een volledige registratie van alle risico's, ook de lage geïdentificeerde risico's.	<ul style="list-style-type: none"> •
	Alle geïdentificeerde risico's worden volledig geregistreerd en systematisch beheerd.	<ul style="list-style-type: none"> •
	De doeltreffendheid van het proces voor het identificeren, beoordelen en beheren van risico's én de risicobeheersmaatregelen worden periodiek beoordeeld en, zo nodig, aangepast.	<ul style="list-style-type: none"> •
VWN5 - geoptimaliseerd	De organisatie heeft een proactieve en geïntegreerde benadering van risicobeheer, waarbij de risico's in de verwerking van persoonsgegevens continu worden gemonitord en aangepast in reactie op veranderingen in zowel de interne organisatie als het externe landschap.	<ul style="list-style-type: none"> •
	Het management controleert en evalueert continu de doeltreffendheid van haar risicobeheersysteem en voert waar nodig verbeteringen door.	<ul style="list-style-type: none"> •

Processen

PR.01 - Operationele processen

Wat	Beschrijving
Domein	Processen
Categorie	Operationele processen
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> risico's voor de rechten en vrijheden van personen indien persoonsgegevens onbedoeld worden gedeeld, ingezien, gewijzigd of worden verloren. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> 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	<p>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.</p> <p>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.</p>
Toetsing	O&P
AVG-UAVG	AVG 24 lid 1
ISO 27701:2019	-
VNG 3.0	2.1
Norea PCF	<ul style="list-style-type: none"> PDI01

PR.01 – Bewijsmateriaal Operationele processen

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	De organisatie heeft geen systematische en gestructureerde aanpak voor het identificeren en documenteren van operationele processen waarin persoonsgegevens worden verwerkt. 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.	<ul style="list-style-type: none"> •
VWN2 - herhaalbaar	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.	<ul style="list-style-type: none"> •
	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.	<ul style="list-style-type: none"> •
VWN3 - bepaald	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.	<ul style="list-style-type: none"> • Documentatie van de methodologie of aanpak die de organisatie gebruikt voor het systematisch identificeren en documenteren van processen waarin persoonsgegevens worden verwerkt. Dit kan inclusief procedures, checklists, of richtlijnen zijn. • Een overzicht van alle processen waarin persoonsgegevens worden verwerkt, met nadruk op processen die als hoog risico zijn geïdentificeerd. Dit kan in de vorm van een register of database (of architectuurplaat) zijn, waarin elk proces is beschreven met betrekking tot de aard van de persoonsgegevens, het doel van de verwerking, en de risicoclassificatie.
	Proceseigenaren zijn aangewezen en zijn verantwoordelijk voor de periodieke evaluatie van de procesbeschrijving en passen deze zo nodig aan.	<ul style="list-style-type: none"> • Een overzicht van aangewezen proceseigenaren voor elk van de processen waarin persoonsgegevens worden verwerkt. • Voorbeelden van documentatie of logs die aantonen dat periodieke evaluaties van de procesbeschrijvingen daadwerkelijk plaatsvinden, inclusief wijzigingen of updates die zijn doorgevoerd als resultaat van deze evaluaties.
VWN4 - beheerst	De organisatie heeft alle operationele processen waarin persoonsgegevens worden verwerkt vastgelegd en beschreven (niet alleen die met hoog risico).	<ul style="list-style-type: none"> •

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	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.	•
	Binnen een vastgesteld interval wordt geëvalueerd of de beschrijving van het proces aansluit bij de praktijk.	•
	Proceseigenaren informeren proactief over de realisatie van uitgevoerde wijzigingen naar aanleiding van evaluaties	•
VWNS - geoptimaliseerd	Het management ziet het belang in van procesmatig werken en het actueel houden van operationele processen en stuurt hier actief op.	•
	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.	•
	Er wordt pro-actief geborgd dat wijzigingen en initiatieven die niet voldoen aan het privacybeleid worden geïdentificeerd en opgelost.	•

PR.02 - Verwerkingsregister inrichten

Wat	Beschrijving
Domein	Processen
Categorie	Verwerkingsregister inrichten (opzet en vastlegging verwerkingen)
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • 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. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>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).</p> <p>In de rol van verwerkingsverantwoordelijke dient het verwerkingsregister per verwerking ten minste de volgende informatie te bevatten:</p> <ul style="list-style-type: none"> • 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
AVG-UAVG	AVG 30

Wat	Beschrijving
ISO 27701:2019	7.2.8
VNG 3.0	2.2
Norea PCF	<ul style="list-style-type: none">• PIA????• PDI02• PDI03• PDI04• DTR01• PPO05• PDI03 <ul style="list-style-type: none">• LRC01• CFR03• DMIO1• URE03• ACD01• ACD02• RRE05

PR.02 – Bewijsmateriaal Verwerkingsregister inrichten

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Er is geen verwerkingsregister of er zijn geen verwerkingen bijgehouden. Wettelijk vereiste onderdelen, rollen voor verwerking (verwerkingsverantwoordelijke, verwerker, gezamenlijke verwerkingsverantwoordelijken) en verwijzingen naar operationele processen zijn niet duidelijk of ontbreken.	•
VWN2 - herhaalbaar	Er is een (gedeeltelijk) ingevuld verwerkingsregister, maar niet alle wettelijk vereiste onderdelen zijn aanwezig.	•
	Voor (sommige) verwerkingen zijn de rollen voor verwerking niet duidelijk of niet gedocumenteerd.	•
	Een deel van de verwerkingen is getoetst aan de privacybeginselen zoals beschreven in art. 5 lid 1 AVG	•
VWN3 - bepaald	Het verwerkingsregister bevat minimaal alle wettelijk vereiste onderdelen (art. 30 lid 1 AVG voor de verwerkingsverantwoordelijk of voor de verwerker lid 2).	<ul style="list-style-type: none"> • Een kopie van of inzage in het actuele verwerkingsregister. • Een checklist of overzicht waarin wordt verwezen naar de wettelijke vereisten uit art. 30 lid 1 en lid 2 AVG en waarin wordt aangegeven waar in het verwerkingsregister aan elk van deze vereisten wordt voldaan.
	Voor elke vastgelegde verwerking is duidelijk wie de verwerkingsverantwoordelijke, de verwerker of de gezamenlijke verwerkingsverantwoordelijken zijn.	<ul style="list-style-type: none"> • Gedetailleerde vermeldingen in het verwerkingsregister die duidelijk maken wie voor elke verwerking de verwerkingsverantwoordelijke, de verwerker, of de gezamenlijke verwerkingsverantwoordelijken zijn. • Overeenkomsten of contracten tussen de verwerkingsverantwoordelijke(n) met verwerkers die de respectievelijke rollen en verantwoordelijkheden definiëren
	De verwerkingen met persoonsgegevens zijn vastgelegd en zijn getoetst aan de privacy beginselen uit art. 5 lid 1 AVG.	<ul style="list-style-type: none"> • Een gedetailleerde lijst of segment van het verwerkingsregister dat specifiek de verwerkingen met hoge risico's toont.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
		<ul style="list-style-type: none"> • Documentatie van beoordelingen of analyses waaruit blijkt dat de verwerkingen met hoge risico's zijn getoetst aan de privacybeginselen uit art. 5 lid 1 AVG. Dit kan bijvoorbeeld in de vorm zijn van een rapport, notulen van vergaderingen of een ander document.
VWN4 - beheerst	Indien de AP inzicht in het verwerkingsregister vraagt, kan dit op eenvoudige wijze worden voorgelegd.	<ul style="list-style-type: none"> •
VWN5 - geoptimaliseerd	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.	<ul style="list-style-type: none"> •
	In het verwerkingsregister staan verwijzingen naar DPIA, verwerkersovereenkomst en andere relevante overeenkomsten.	<ul style="list-style-type: none"> •
	Het register bevat volledige en actuele verwijzingen naar alle operationele processen waarbinnen persoonsgegevens worden verwerkt.	<ul style="list-style-type: none"> •

PR.03 - Verwerkingsregister actualiseren

Wat	Beschrijving
Domein	Processen
Categorie	Verwerkingsregister actualiseren
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • 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. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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
AVG-UAVG	AVG 30
ISO 27701:2019	7.2.8
VNG 3.0	2.2
Norea PCF	<ul style="list-style-type: none"> • PDIO4 • DTR01

PR.03 – Bewijsmateriaal Actualiseren

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Er is geen duidelijke procedure voor het bijhouden van nieuwe en gewijzigde verwerkingen in het verwerkingsregister.	<ul style="list-style-type: none"> •
VWN2 - herhaalbaar	Er is een informele procedure voor het bijhouden van nieuwe en gewijzigde verwerkingen in het verwerkingsregister, maar deze wordt niet consequent toegepast.	<ul style="list-style-type: none"> •
	Het verwerkingsregister is niet up-to-date omdat wijzigingen in verwerkingen niet altijd tijdig in het verwerkingsregister worden opgenomen	<ul style="list-style-type: none"> •
	De verantwoordelijkheden voor het bijhouden van het verwerkingsregister zijn toegewezen, maar worden niet actief opgepakt.	<ul style="list-style-type: none"> •
VWN3 - bepaald	Er is een vastgestelde procedure die definieert hoe en wanneer nieuwe en gewijzigde verwerkingen in het verwerkingsregister worden opgenomen.	<ul style="list-style-type: none"> • Een kopie van de vastgestelde (wijzigings-)procedure of richtlijn die het proces van toevoegen en wijzigen in het verwerkingsregister beschrijft. • Documentatie van recente gevallen waarin deze procedure is gevolgd (bijvoorbeeld ingevulde formats, screenshots of e-mailcorrespondentie).
	Bij wijzigingen wordt opnieuw getoetst of de verwerking in overeenstemming is met de privacybeginselen uit art. 5 lid 1 AVG.	<ul style="list-style-type: none"> • Documentatie of checklists die laten zien dat bij wijzigingen in het verwerkingsregister opnieuw is getoetst aan de privacy beginselen uit art. 5 lid 1 AVG. Bijvoorbeeld middels een uitgevoerde (pre-)DPIA Check. • Documentatie van recente gevallen waarin deze procedure is gevolgd (bijvoorbeeld ingevuld format, screenshots of e-mailcorrespondentie).
	Er is vastgesteld met welke frequentie het verwerkingsregister wordt beoordeeld op volledigheid en actualiteit, en welke functionaris verantwoordelijk is voor deze beoordeling.	<ul style="list-style-type: none"> • Een formeel document, richtlijn of beleidsstuk waarin de frequentie van beoordeling en de verantwoordelijke functionaris zijn vastgelegd. • Verslagen of logs van recente beoordelingen van het verwerkingsregister.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	Wijzigingen en nieuwe initiatieven waarbij persoonsgegevens worden verwerkt, worden direct in het register opgenomen.	<ul style="list-style-type: none"> • Wijzigingslogs, ingevulde formats of historie van het verwerkingsregister waaruit blijkt dat recente of nieuwe initiatieven zijn opgenomen.
VWN4 - beheerst	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.	<ul style="list-style-type: none"> •
VWN5 - geoptimaliseerd	De organisatie heeft een tool ingezet voor het bijhouden en auditen van het verwerkingsregister.	<ul style="list-style-type: none"> •

PR.04 – Risico-inschatting (pre-DPIA)

Wat	Beschrijving
Domein	Processen
Categorie	Identificatie van risico's (met behulp van pre-DPIA's)
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> risico's voor de rechten en vrijheden van personen door onvoldoende of verkeerde maatregelen om de risico's te mitigeren. <p>Voor de organisatie</p> <ul style="list-style-type: none"> 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	<p>De criteria die bepalen of een verwerking een hoog risico vormt voor betrokkenen zijn opgenomen in de lijsten van de AP en EDPB:</p> <ul style="list-style-type: none"> AP, wanneer een DPIA? Guideline DPIA EDPB <p>Voor VWN3.a en VWN3.b geldt dat de methode met het in BL.03 beschreven risicobeoordelingsproces moet overeenkomen.</p>
Toetsing	O&P
AVG-UAVG	AVG 35
ISO 27701:2019	7.2.5
VNG 3.0	2.3
Norea PCF	<ul style="list-style-type: none"> PIA01 RMA03 PBD01 LRC01

PR.04 – Bewijsmateriaal Risico-inschatting (pre-DPIA)

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	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. Er is geen systematische beoordeling van alle verwerkingen om te bepalen of deze een hoog risico kunnen opleveren.	•
VWN2 - herhaalbaar	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.	•
	Niet alle verwerkingen zijn beoordeeld op een mogelijk hoog risico.	•
	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	Er is een methode/procedure vastgesteld om voor alle nieuwe en gewijzigde verwerkingen te bepalen of deze mogelijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.	<ul style="list-style-type: none"> • Een kopie van de vastgestelde methode, richtlijn of procedure voor risicobeoordeling van nieuwe en gewijzigde verwerkingen. Bijvoorbeeld een procedure uitvoeren pre-DPIA of DPIA Check. • Eventuele trainings- of voorlichtingsmateriaal dat is gebruikt om het personeel bekend te maken met deze procedure.
	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.	<ul style="list-style-type: none"> • Documentatie van recente gevallen waarin de methode of procedure is toegepast, zoals risicobeoordelingsrapporten (bijvoorbeeld (pre-)DPIA Check) of notulen van vergaderingen.
	Alle verwerkingen zijn beoordeeld op mogelijk hoog risico en deze zijn als zodanig aangemerkt in het verwerkingsregister.	<ul style="list-style-type: none"> • Een uittreksel of screenshot van het verwerkingsregister waarin verwerkingen zijn aangemerkt als "hoog risico".
	De analyse die ten grondslag ligt aan de beslissing of een verwerking een hoog risico kan opleveren, is gedocumenteerd.	<ul style="list-style-type: none"> • Kopieën van risicoanalyses of beoordelingen die zijn uitgevoerd voor specifieke verwerkingen.
VWN4 - beheerst	Verwerkingen die waarschijnlijk een hoog risico inhouden, worden proactief geïdentificeerd en beheerd.	•

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	De procedure voor het identificeren van hoog risico verwerkingen wordt periodiek geëvalueerd en zo nodig verbeterd.	•
	De analyse en documentatie van het besluit of een verwerking een hoog risico kan opleveren, is gemakkelijk te vinden en toegankelijk.	•
VWN5 - geoptimaliseerd	Het identificeren van hoog risico verwerkingen is volledig geïntegreerd in de operationele processen van de organisatie.	•
	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).	•
	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.	•

PR.05 - DPIA's

Wat	Beschrijving
Domein	Processen
Categorie	DPIA's
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen door onvoldoende of verkeerde maatregelen om de risico's te mitigeren. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>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).</p> <p>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:</p> <ul style="list-style-type: none"> • AP uitvoeren DPIA <p>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.</p>
Toetsing	O&P
AVG-UAVG	AVG 35 AVG 36
ISO 27701:2019	5.2.2 7.2.5
VNG 3.0	2.4
Norea PCF	<ul style="list-style-type: none"> • PIA01 • PIA02 • PIA04 • PIA05 <ul style="list-style-type: none"> • PIA06 • RMA05 • RRE04 • RRE05

PR.05 – Bewijsmateriaal DPIA's

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Er is geen formele procedure vastgesteld voor het uitvoeren van DPIA's op nieuwe en sterk gewijzigde verwerkingen die mogelijk een hoog risico inhouden. De FG wordt (nog) niet betrokken of om advies gevraagd bij het uitvoeren van DPIA's.	•
VWN2 - herhaalbaar	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.	•
	DPIA-rapporten worden wel opgesteld, maar voldoen niet altijd aan de wettelijke vereisten.	•
	Niet alle hoog-risico verwerkingen zijn onderworpen aan een DPIA.	•
	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	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.	<ul style="list-style-type: none"> • Een kopie van de vastgestelde DPIA-methode. • Documentatie van recente gevallen waarin deze methode is gevolgd (bijvoorbeeld wijzigingslogs, screenshots of e-mailcorrespondentie).
	Er is een procedure vastgesteld voor het opvolgen (behandelen of accepteren) van risico's die in een DPIA zijn geïdentificeerd.	<ul style="list-style-type: none"> • Een kopie van de vastgestelde procedure voor het opvolgen van DPIA-resultaten. • Voorbeelden van situaties waarin de procedure is gevolgd, zoals documentatie over de opvolging van specifieke risico's.
	DPIA-rapporten worden opgesteld volgens een gestandaardiseerd format dat voldoet aan de wettelijke vereisten.	<ul style="list-style-type: none"> • Een kopie van het gestandaardiseerde DPIA-format. • Voorbeelden van recent uitgevoerde DPIA's opgesteld in het genoemde format. • Een link tussen het format en de wettelijke vereisten.
	Alle hoog-risico verwerkingen zijn onderworpen aan een DPIA.	<ul style="list-style-type: none"> • Een lijst van alle hoog-risico verwerkingen en bijbehorende DPIA-rapporten, incl. FG-advies.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	Er is een standaardprocedure voor het documenteren van afwijkingen van het advies van de FG. Deze procedure wordt consequent gevolgd.	<ul style="list-style-type: none"> Een kopie van de vastgestelde procedure voor het documenteren en onderbouwing van afwijkingen van het advies van de FG. Documentatie of notulen waaruit blijkt dat de procedure consequent wordt gevolgd, met, indien van toepassing, voorbeelden van daadwerkelijke afwijkingen.
	De DPIA-rapportages zijn makkelijk vindbaar.	<ul style="list-style-type: none"> Een beschrijving van waar en hoe de DPIA-rapportages worden opgeslagen. Een demonstratie of screenshots van de zoek- en toegangsmogelijkheden voor deze rapportages in het systeem.
VWN4 - beheerst	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.	<ul style="list-style-type: none">
	DPIA's worden minstens elke 36 maanden opnieuw beoordeeld.	<ul style="list-style-type: none">
	Bij een afwijking van een FG-advies, legt het management onderbouwd vast waarom afgeweken is van het advies.	<ul style="list-style-type: none">
	In gevallen waar een geïdentificeerd risico niet gemitigeerd of geaccepteerd wordt, wordt dit expliciet gedocumenteerd en uitgelegd.	<ul style="list-style-type: none">
	Er is een overzicht van en inzicht in de uitgevoerde DPIA's, inclusief de data waarop deze zijn uitgevoerd of herzien.	<ul style="list-style-type: none">
	Periodiek wordt de effectiviteit van de DPIA-procedure geëvalueerd om continue verbetering te bevorderen.	<ul style="list-style-type: none">
VWN5 - geoptimaliseerd	Er is actieve betrokkenheid van het hoogste management bij het DPIA-proces, vooral wanneer er wordt afgeweken van het advies van de FG.	<ul style="list-style-type: none">
	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.	<ul style="list-style-type: none">

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	De organisatie heeft de effectiviteit en efficiëntie van haar DPIA-proces geoptimaliseerd, bijvoorbeeld door gebruik te maken van automatisering of geavanceerde tools.	<ul style="list-style-type: none">•
	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.	<ul style="list-style-type: none">•

PR.06 - Privacy by Design

Wat	Beschrijving
Domein	Processen
Categorie	Gegevensbescherming door ontwerp en standaardinstellingen (Privacy by Design & Privacy by Default)
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen door onvoldoende of verkeerde Privacy by Design/Privacy by Default maatregelen. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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
AVG-UAVG	AVG 25 lid 1
ISO 27701:2019	7.4
VNG 3.0	6.2 6.3
Norea PCF	<ul style="list-style-type: none"> • PBD01 • PBD02 • PBD03 • RMA05

PR.06 – Bewijsmateriaal Privacy by Design

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	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. Risicomanagement met betrekking tot privacy wordt sporadisch toegepast en stelt weinig tot geen eisen aan externe partijen.	•
VWN2 - herhaalbaar	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.	•
	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.	•
	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	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.	<ul style="list-style-type: none"> • Een kopie van de gedocumenteerde eisen en beginselen. • Voorbeelden van projecten of initiatieven waarbij deze eisen en beginselen vanaf het begin af aan zijn toegepast.
	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.	<ul style="list-style-type: none"> • Documentatie of checklists die worden gebruikt voor de beoordeling van privacyrisico's bij inkoop- of ontwikkel-trajecten. • Voorbeelden van recente beoordelingen.
	Bij samenwerking met externe partijen stelt de organisatie consequent eisen op het gebied van Privacy by Design.	<ul style="list-style-type: none"> • Kopieën van contracten, convenanten of overeenkomsten met externe partijen waarin de eisen zijn vastgelegd.
	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.	<ul style="list-style-type: none"> • Documentatie of handleidingen van de configuratie waaruit dit principe blijkt.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
		<ul style="list-style-type: none"> • Screenshots of demonstraties van systemen waarin Privacy by Default is toegepast.
	<p>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.</p>	<ul style="list-style-type: none"> • Een kopie van de gedocumenteerde richtlijnen.
VWN4 - beheerst	<p>Privacy by Default is consequent geïntegreerd als een standaard aspect van de configuratie voor alle toepassingen, diensten en producten.</p>	<ul style="list-style-type: none"> •
	<p>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.</p>	<ul style="list-style-type: none"> •
	<p>De organisatie stelt strikte eisen aan externe partijen voor het toepassen van adequaat privacy risicomanagement. Deze eisen worden periodiek gecontroleerd en, indien nodig, verbeterd.</p>	<ul style="list-style-type: none"> •
	<p>De privacy-ricobeoordeling 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.</p>	<ul style="list-style-type: none"> •
	<p>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".</p>	<ul style="list-style-type: none"> •
VWN5 - geoptimaliseerd	<p>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.</p>	<ul style="list-style-type: none"> •
	<p>Strikte eisen met betrekking tot privacyrisicomanagement, zowel voor Privacy by Design als Privacy by Default, zijn verankerd in de contractuele relaties van de organisatie.</p>	<ul style="list-style-type: none"> •

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	<p>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.</p>	<ul style="list-style-type: none">•

PR.07 - Bewaren en vernietigen

Wat	Beschrijving
Domein	Processen
Categorie	Bewaar- en vernietigingsbeleid
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> risico's voor de rechten en vrijheden van personen als gevolg van hergebruik van persoonsgegevens voor andere dan de oorspronkelijke doelen. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> 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	<p>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.</p> <p>Voor persoonsgegevens die niet in de selectielijst zijn opgenomen en waarvoor geen wettelijke bewaartermijnen gelden, zijn beleidsregels opgenomen.</p> <p>Het 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.</p> <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> EDPS - anonimiseren
Toetsing	O&P
AVG-UAVG	AVG 5 lid 1 sub e c
ISO 27701:2019	7.4
VNG 3.0	2.5
Norea PCF	<ul style="list-style-type: none"> PPO05 DRE01 DRE02 DDA01 DDA02 ENC03

PR.07 – Bewijsmateriaal Bewaren en vernietigen

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Er is geen vastgesteld beleid voor het verwijderen en anonimiseren van gegevens ('bewaarbeleid' of 'vernietigingsbeleid'). Het verwijderen of anonimiseren van persoonsgegevens vindt niet, onregelmatig en/of inconsistent (bijvoorbeeld afhankelijk van individuen of incidenten) plaats.	•
VWN2 - herhaalbaar	Er is informeel beleid of beleid op decentraal niveau voor het verwijderen en/of anonimiseren van gegevens.	•
	Voor algemene, veelvoorkomende gevallen zijn er procedures voor het verwijderen van gegevens, maar voor meer specifieke gevallen ontbreken deze procedures.	•
VWN3 - bepaald	Er is beleid vastgesteld voor het verwijderen en/of anonimiseren van gegevens.	<ul style="list-style-type: none"> • Een kopie van het vastgestelde bewaartermijnen-beleid. • Notulen of andere documentatie waarin het besluit tot vaststelling van het beleid is gedocumenteerd. • Selectielijst Hoger Onderwijs (bewaartermijnen) wordt gehanteerd en toegepast.
	De processen om persoonsgegevens te verwijderen of te anonimiseren zijn gedocumenteerd.	<ul style="list-style-type: none"> • Kopieën van de gedocumenteerde processen.
	Persoonsgegevens die niet meer nodig zijn worden tijdig verwijderd of geanonimiseerd, conform het beleid.	<ul style="list-style-type: none"> • Logging of rapportages die de daadwerkelijke verwijdering of anonimisering van gegevens aantonen. • Steekproeven, controles of audits waaruit blijkt dat het beleid wordt nageleefd.
	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.	<ul style="list-style-type: none"> • Kopieën van de specifieke procedures. • Een overzicht van de gegevenssoorten waarvoor deze procedures gelden. • Voorbeelden van situaties waarin deze procedures zijn toegepast.
VWN4 - beheerst	Het beleid en de procedures voor het verwijderen en anonimiseren van gegevens worden consequent toegepast.	•

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	Het beleid en de procedures voor het verwijderen en anonimiseren worden periodiek geëvalueerd en zo nodig aangepast.	•
	Het beleid besteedt aandacht aan het verwijderen/anonimiseren bij leveranciers (bijvoorbeeld SaaS applicaties of applicaties die anderszins persoonsgegevens verwerken).	•
	Periodiek wordt gecontroleerd of applicaties daadwerkelijk verwijderen of anonimiseren conform het bewaar- en vernietigingsbeleid.	•
	Waar mogelijk wordt het verwijderen of anonimiseren van persoonsgegevens geautomatiseerd uitgevoerd.	•
VWN5 - geoptimaliseerd	Het beleid en de procedures voor het verwijderen en anonimiseren van gegevens zijn volledig, transparant, en worden gezien als krachtige hulpmiddelen binnen de organisatie.	•
	Het is mogelijk een geautomatiseerd bewaar- en vernietigingsregime toe te passen op persoonsgegevens, bij voorkeur ook gekoppeld aan doelen.	•
	Deze geautomatiseerde systemen zijn volledig geïntegreerd in de operationele processen van de organisatie.	•

Organisatorische inbedding

OI.01 – FG

Wat	Beschrijving
Domein	Organisatorische inbedding
Categorie	Aanwijzing en positie functionaris gegevensbescherming
Beschrijving risico	<p>Als de FG-rol niet correct of volledig is ingebed binnen de organisatie kan dit de effectiviteit van haar toezichhoudende 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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> risico's voor de rechten en vrijheden van personen als gevolg van het ontbreken van onafhankelijk intern toezicht door de FG. <p>Voor de organisatie: gebrek aan vertrouwen. dwangmaatregelen of boetes opgelegd door de toezichthouder.</p>
Beheerdoelstelling	De organisatie heeft een functionaris gegevensbescherming (FG) aangesteld /aangewezen en zodanig onafhankelijk gepositioneerd dat deze effectief toezicht kan houden.
Toelichting	<p>Zie o.a. de website van de AP over de positionering van de FG:</p> <ul style="list-style-type: none"> AP - positionering van de FG <p>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.</p>
Toetsing	O
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	<ul style="list-style-type: none"> RRE04 SCO01 SCO04

OI.01 – Bewijsmateriaal FG

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	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. De rol en verantwoordelijkheden van de FG zijn niet gedefinieerd. De contactgegevens van de FG ontbreken en zijn niet (makkelijk) vindbaar. De FG is niet betrokken bij opleiding en bewustwordingsprogramma's.	•
VWN2 - herhaalbaar	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.	•
	De FG heeft beperkte tijd, middelen of ondersteuning (van het management) om zijn of haar taken te vervullen.	•
	De betrokkenheid van de FG bij opleiding en bewustwordingsprogramma's is minimaal en/of gebeurt ad hoc.	•
VWN3 - bepaald	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.	<ul style="list-style-type: none"> • Functieomschrijving of aanstellingsbrief waarin de onafhankelijkheid en verantwoordelijkheden van de FG zijn vastgelegd. Dit kan ook in het P-Beleid beschreven staan. • Er is een FG reglement waarin minimaal de AVG vereisten (art 37 t/m 39) in opgenomen staan.
	De FG heeft geen taken of verplichtingen die kunnen leiden tot een belangenconflict bij de uitvoering van hun taken als FG.	<ul style="list-style-type: none"> • Een overzicht van de taken en verplichtingen van de FG. • P-Beleid en/of FG Reglement
	De FG heeft voldoende tijd en middelen om zijn of haar taken effectief uit te voeren.	<ul style="list-style-type: none"> • Jaarplanning, activiteitenplan of andere documentatie waarin de toegewezen tijd en middelen voor de FG zijn vastgelegd. • FG jaarverslag, waarin dit onderdeel beschreven staat.
	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 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.	<ul style="list-style-type: none"> • Kopie van het functieprofiel en/of FG Reglement. • Checklists of beoordelingscriteria gebruikt tijdens de selectieprocedure, waaruit blijkt dat er rekening gehouden worden met artikel 37 lid 5. • Aanstellingsbesluit / Opdrachtbeschrijving / Overeenkomst van Opdracht is vindbaar.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	De FG wordt tijdig betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens waaronder advies bij iedere DPIA.	<ul style="list-style-type: none"> • Logboek, verslagen, besluiten, opleggers of notulen waaruit blijkt dat de FG tijdig is geconsulteerd bij relevante aangelegenheden.
	Contactgegevens van de FG zijn actueel, beschikbaar, en makkelijk te vinden.	<ul style="list-style-type: none"> • Screenshots of links naar de contactpagina van de organisatie waar de gegevens van de FG te vinden zijn. Zodoende zowel intern als extern kenbaar gemaakt. • Opgenomen in de privacyverklaring.
	De FG is betrokken bij opleiding en bewustwordingsprogramma's op het gebied van privacy.	<ul style="list-style-type: none"> • Documenten waaruit de betrokkenheid van de FG blijkt. • Notulen van trainingssessies of bijeenkomsten waarbij de FG aanwezig was.
	De FG brengt rechtstreeks verslag uit aan het hoogste management doet over de naleving van de AVG door de organisatie.	<ul style="list-style-type: none"> • Notulen of agenda's van vergaderingen tussen de FG en het hoogste management.
	De FG stemt periodiek af met het hoogste management binnen de organisatie.	<ul style="list-style-type: none"> • Kopieën van de verslagen, adviezen of aanbevelingen die door de FG zijn opgesteld. • Correspondentie of e-mails waarin het verslag, of advies wordt besproken met het hoogste management
VWN4 - beheerst	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.	<ul style="list-style-type: none"> •
	De FG voert periodiek zelfevaluaties uit en betreft 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, betreft de FG het management om samen tot een oplossing te komen.	<ul style="list-style-type: none"> •
	De contactgegevens van de FG zijn niet alleen beschikbaar, maar worden ook proactief gecommuniceerd naar relevante partijen.	<ul style="list-style-type: none"> •
	De FG brengt periodiek verslag uit aan het bestuur over de naleving van de AVG door de organisatie.	<ul style="list-style-type: none"> •

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN5 - geoptimaliseerd	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.	•
	De FG brengt regelmatig ongevraagd advies uit; het bestuur past deze adviezen toe of legt vast waarom daarvan afgeweken wordt.	•
	De aanstelling, verantwoordelijkheden, en middelen voor de FG zijn optimaal en worden continu verbeterd.	•
	De FG speelt een strategische rol in het ontwikkelen en leveren van opleiding en bewustwordingsprogramma's.	•
	De FG is betrokken bij opleiding en bewustwordingsprogramma's op het gebied van privacy.	•

01.02 – Privacyteam

Wat	Beschrijving
Domein	Organisatorische inbedding
Categorie	Privacyorganisatie
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen door verkeerde besluitvorming omtrent de bescherming van persoonsgegevens. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>Voorbeelden van relevante stakeholders zijn de archivaris en management.</p> <p>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).</p> <p>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.</p>
Toetsing	0
AVG-UAVG	-
ISO 27701:2019	6.3
VNG 3.0	3.1
Norea PCF	<ul style="list-style-type: none"> • RRE04 - SC004 - LRC01

OI.02 – Bewijsmateriaal Privacyteam

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Er is geen of weinig (juridische) kennis over. Er is geen aanvullende privacyfunctionaris (of andere privacydeskundige naast de FG).	•
VWN2 - herhaalbaar	Er zijn één of enkele privacy officers (of adviseurs) die actief bijdragen aan het oplossen van (complexvraagstukken over privacy en de bescherming van persoonsgegevens).	•
	Er is incidenteel en/of informeel overleg en afstemming tussen de privacy- en informatiebeveiligingsfunctionarissen.	•
VWN3 - bepaald	Er is een (virtueel) privacyteam waarbij de FG, privacy officer(s) en eventuele decentrale privacy ambassadeurs/coördinatoren zijn aangesloten.	• Organogram of lijst waaruit de samenstelling van het privacyteam blijkt.
	Het privacyteam werkt nauw samen met de informatiebeveiligingsfunctionarissen om vraagstukken rond informatiebeveiliging speelt, zoveel mogelijk gezamenlijk of althans in overleg, op te lossen.	<ul style="list-style-type: none"> • Planning, Notulen of actiepunten van gezamenlijke overlegmomenten tussen het privacyteam en informatiebeveiligingsfunctionarissen. • Betrokkenheid (C)ISO bij DPIA uitvoering en privacy officer bij BIV-classificatie (bijvoorbeeld adviezen/input)
	Medewerkers kunnen eenvoudig en makkelijk contact opnemen met het privacyteam. Het privacyteam reageert binnen een vooraf vastgestelde maximale reactietijd op vragen uit de organisatie.	<ul style="list-style-type: none"> • Communicatierichtlijnen of beleid waarin staat beschreven hoe medewerkers het privacyteam kunnen benaderen en wat de verwachte reactietijd is. • Screenshots van Intranet- of Internetpagina (bijvoorbeeld tegel, topdesk of formulier)
	Het privacyteam heeft periodiek overleg om de werkzaamheden te bespreken en activiteiten af te stemmen, met betrokkenheid van relevante stakeholders.	• Overlegstructuur, notulen, agenda's of bijeenkomstuitnodigingen waaruit blijkt dat er periodieke meetings zijn met relevante stakeholders.
VWN4 - beheerst	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.	•

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN5 - geoptimaliseerd	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.	•
	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.	•
	Privacyfunctionarissen werken proactief samen met andere stakeholders voor de continue verbetering van de privacygerelateerde werkzaamheden.	•

01.03 – Betrokkenheid

Wat	Beschrijving
Domein	Organisatorische inbedding
Categorie	Betrokkenheid medezeggenschap
Beschrijving risico	<p>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.</p> <p>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:</p> <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>Geraadpleegde bronnen:</p> <ul style="list-style-type: none"> • open.overheid (pagina 9 alinea V) • Tweede Kamer (pagina 7 eerste rij)
Toetsing	0
AVG-UAVG	-
ISO 27701:2019	6.3
VNG 3.0	3.3
Norea PCF	

OI.3 – Bewijsmateriaal Betrokkenheid

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Het medezeggenschapsorgaan wordt niet of slechts informeel betrokken bij onderwerpen over de omgang met en bescherming van persoonsgegevens.	•
VWN2 - herhaalbaar	Het medezeggenschapsorgaan wordt ad hoc betrokken bij onderwerpen over de omgang met en bescherming van persoonsgegevens. De informatievoorziening aan het medezeggenschapsorgaan is willekeurig en ongestructureerd.	•
VWN3 - bepaald	Er is een gedocumenteerd proces dat specificeert hoe en wanneer het medezeggenschapsorgaan geïnformeerd en betrokken wordt bij wettelijke taken op het gebied van privacy.	<ul style="list-style-type: none"> • Een formele procedure of beleidsdocument dat de stappen, timings, en betrokkenen beschrijft over hoe het medezeggenschapsorgaan wordt geïnformeerd en betrokken bij besluiten omtrent persoonsgegevens. • Documentatie (zoals e-mails of vergadernotulen) waaruit blijkt dat het medezeggenschapsorgaan daadwerkelijk op de beschreven manier is betrokken.
	Instemmingsprocedures zijn duidelijk gedocumenteerd en worden gevolgd waar wettelijk vereist.	<ul style="list-style-type: none"> • Een formele procedure of richtlijn die de instemmingsprocedures beschrijft, inclusief wanneer deze procedures vereist zijn, hoe instemming wordt verkregen, en wie erbij betrokken is. • Bewijs van naleving, zoals ondertekende documenten van instemming of notulen van vergaderingen waarbij instemmingsbeslissingen zijn genomen.
VWN4 - beheerst	Het medezeggenschapsorgaan wordt actief geïnformeerd en communicatie daaromheen worden periodiek geëvalueerd en waar nodig aangepast.	•

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN5 - geoptimaliseerd	<p>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.</p> <p>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.</p> <p>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.</p>	<ul style="list-style-type: none">•

01.04 – Bewustwording

Wat	Beschrijving
Domein	Organisatorische inbedding
Categorie	Bewustwording
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen door verkeerde besluitvorming omtrent de bescherming van persoonsgegevens <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p>
Toetsing	O&P
AVG-UAVG	AVG 39 1b AVG 24 lid 1
ISO 27701:2019	6.4.2.2
VNG 3.0	3.4
Norea PCF	<ul style="list-style-type: none"> • SCO02 • SCO03 • RRE05 • SAT01 <ul style="list-style-type: none"> • SAT02 • SAT03 • SCO02

OI.04 – Bewijsmateriaal Bewustwording

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Er zijn geen activiteiten of initiatieven gedefinieerd of uitgevoerd om het bewustzijn over privacy te vergroten. Medewerkers worden bij indiensttreding niet geïnformeerd over privacy. Onderwijsdeelnemers worden niet geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens.	•
VWN2 - herhaalbaar	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).	•
	Onderwijsdeelnemers worden op incidentele basis geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens.	•
VWN3 - bepaald	Er is een programma/opleidingsplan waarin medewerkers bij indiensttreding en, indien nodig, tijdens het dienstverband worden geïnformeerd over privacy en de bescherming van persoonsgegevens.	<ul style="list-style-type: none"> • Een gedocumenteerd opleidingsplan of programma waarin specifiek de inhoud en frequentie van privacy trainingen of e-learnings wordt beschreven. • Aanmeldingsformulieren, certificaten of andere documentatie waaruit blijkt dat medewerkers daadwerkelijk de training hebben gevolgd. Dit kan ook een onderdeel zijn van het introductieprogramma
	Medewerkers zijn goed geïnformeerd over hun verantwoordelijkheden met betrekking tot privacy en de bescherming van persoonsgegevens en handelen daarnaar.	<ul style="list-style-type: none"> • Interne beleidsdocumenten over privacy-verantwoordelijkheden van medewerkers • Trainingsmateriaal en deelnamelijsten voor privacy-opleidingen • Incident- of klachtenregistraties die laten zien dat medewerkers privacy-incidenten correct hebben afgehandeld, zoals beschrijvingen van hoe het incident is opgepakt volgens protocol
	Onderwijsdeelnemers worden op een planmatige manier geïnformeerd over het belang van privacy en de bescherming van persoonsgegevens.	<ul style="list-style-type: none"> • Een gedocumenteerd plan dat beschrijft hoe en wanneer onderwijsdeelnemers worden geïnformeerd over privacy en gegevensbescherming. • Bewijs van daadwerkelijke implementatie, zoals lesmateriaal, presentaties, communicatie, campagnes of andere middelen die worden gebruikt om onderwijsdeelnemers te informeren.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN4 - beheerst	Voor alle niveaus worden de vaardigheidsvereisten systematisch bijgehouden; deskundigheidsbevordering is gewaarborgd in alle kritieke gebieden en certificering op het gebied van privacy skills wordt aangemoedigd.	•
	Periodiek wordt geëvalueerd of met de trainingen de beoogde resultaten worden behaald en waar nodig worden trainingen en of het trainingsprogramma aangepast.	•
	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	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.	•
	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.	•
	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.	•

Rechten van betrokkenen

RB.01 - Rechten van betrokkenen

Wat	Beschrijving
Domein	Rechten van betrokkenen
Categorie	Afhandeling rechten van betrokkenen
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> risico's voor de rechten en vrijheden van personen door onvolledige of trage afhandeling van de rechten van betrokkene <p>Voor de organisatie:</p> <ul style="list-style-type: none"> 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
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	<ul style="list-style-type: none"> DAR01 DAR03 DAR04 DCR01 DCR03 DCR04 DDR01 DDR02 DDR04 URE02

RB.01 – Bewijsmateriaal Rechten van betrokkenen

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	De organisatie heeft geen technische of organisatorische maatregelen genomen om de rechten van betrokkenen te waarborgen. Er is geen proces voor het indienen en afhandelen van verzoeken. Medewerkers herkennen AVG-verzoeken niet en weten niet naar wie ze deze moeten doorsturen voor afhandeling. 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	De organisatie heeft voor de afhandeling van rechten van betrokkenen enkele technische en organisatorische maatregelen genomen, maar de implementatie is onvolledig en inconsistent.	•
	Verzoeken kunnen zowel analoog als digitaal worden ingediend, maar de communicatie hierover is gebrekkig.	•
	Er zijn basisprocedures voor de afhandeling van verzoeken, maar de naleving van termijnen is inconsistent en/of de communicatie met betrokkenen is gebrekkig.	•
	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	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; 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.	• Een kopie van de gedocumenteerde procedure die alle genoemde elementen bevat.
	Verzoeken kunnen zowel analoog als digitaal worden ingediend en dit proces is duidelijk gecommuniceerd naar betrokkenen.	• Documentatie of schermafbeeldingen van het digitale indieningsproces.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
		<ul style="list-style-type: none"> Kopieën van communicatiemiddelen waarin het indieningsproces wordt uitgelegd, zoals flyers, e-mails of website-instructies.
	Betrokkenen ontvangen altijd een ontvangstbevestiging van hun verzoeken en worden tijdig geïnformeerd over de status van de behandeling.	<ul style="list-style-type: none"> Voorbeelden van verzonden ontvangstbevestigingen of een automatisch gegenereerd e-mailbericht. Logboeken of andere registraties/'tickets' die aantonen dat betrokkenen op de hoogte worden gehouden van de status van hun verzoek
	Applicaties en systemen bevatten voldoende mogelijkheden om de rechten van betrokkenen effectief uit te voeren.	<ul style="list-style-type: none"> Technische documentatie, handleidingen, schermafdrucken van applicaties en systemen waaruit blijkt dat deze functionaliteiten bevatten voor de afhandeling van de rechten van betrokkenen. Bijvoorbeeld middels 'self-service' mogelijkheid Voorbeelden van daadwerkelijke uitvoeringen of acties (of schermafbeeldingen) binnen de systemen naar aanleiding van verzoeken.
	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.	<ul style="list-style-type: none"> Een (geanonimiseerde) lijst of database van eerder behandelde verzoeken met bijbehorende beslissingen en afhandelingsdata. Register Rechten van Betrokkenen (actueel en beheert) Richtlijnen of procedures over hoe deze registratie wordt bijgehouden en gebruikt.
	Medewerkers zijn goed getraind in het herkennen van AVG-verzoeken en weten precies naar wie ze deze moeten doorsturen.	<ul style="list-style-type: none"> Trainingsschema's of curricula over AVG en gerelateerde onderwerpen. Bewijs van deelname, zoals certificaten of aanmeldingsformulieren, waaruit blijkt dat medewerkers de training hebben gevolgd.
VWN4 - beheerst	Verzoeken van betrokkenen worden tijdig afgehandeld en er is een proces voor het signaleren, melden en analyseren van vertragingen.	<ul style="list-style-type: none">
	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.	<ul style="list-style-type: none">
	De organisatie houdt een gedetailleerde registratie bij van eerder behandelde verzoeken en gebruikt deze om nieuwe verzoeken consistent en nauwkeurig te toetsen.	<ul style="list-style-type: none">
VWN5 - geoptimaliseerd	Alle applicaties en systemen bevatten geavanceerde en effectieve mogelijkheden voor de uitvoering van de rechten van betrokkenen.	<ul style="list-style-type: none">

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	Er worden benchmarks (bijvoorbeeld binnen de onderwijssector) uitgevoerd om te toetsen of de uitvoering van rechten van betrokkenen aansluit op wat algemeen gangbaar is.	<ul style="list-style-type: none">•

RB.02 – Informatieplicht

Wat	Beschrijving
Domein	Rechten van betrokkenen
Categorie	Informatieplicht
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen door een gebrek aan informatie over de verwerking van zijn/haar persoonsgegevens. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>De privacyverklaring moet deze criteria en onderwerpen bevatten:</p> <ul style="list-style-type: none"> • 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 en 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. <p>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.</p>
Toetsing	O&P
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	<ul style="list-style-type: none"> • PST01

RB.02 – Bewijsmateriaal Informatieplicht

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Betrokkenen worden niet of onvoldoende geïnformeerd over hun rechten. Er is geen informatie verstrekt aan betrokkenen van wie de persoonsgegevens niet rechtstreeks zijn verkregen. De organisatie heeft geen algemene privacyverklaring gepubliceerd op de website of in applicaties en formulieren. Er is geen cookiebeleid of uniforme afspraken over de toepassing van cookies. Bezoekers van de website worden niet geïnformeerd over het gebruik van cookies.	•
VWN2 - herhaalbaar	Betrokkenen worden geïnformeerd, maar de communicatie is soms niet adequaat of te laat.	•
	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.	•
	De informatie over de verwerking van persoonsgegevens in applicaties en formulieren is beperkt en niet altijd duidelijk.	•
	Betrokkenen van wie de persoonsgegevens niet rechtstreeks zijn verkregen, worden niet altijd of niet volledig geïnformeerd.	•
	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	Er is beleid vastgesteld over het informeren van betrokkenen, inclusief de timing van de informatieverstrekking.	<ul style="list-style-type: none"> • Een kopie van het beleidsdocument waarin het informeren van betrokkenen is opgenomen, inclusief de timing van de informatieverstrekking. • Procedurebeschrijving Rechten van Betrokkenen
	Betrokkenen worden adequaat en tijdig geïnformeerd in overeenstemming met de beginselen van behoorlijke en transparante verwerking.	<ul style="list-style-type: none"> • Voorbeelden van communicatiematerialen, zoals e-mails of brieven, waaruit blijkt dat betrokkenen zijn geïnformeerd. • Een overzicht van data en tijden waarop communicaties zijn verzonden.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	Personen van wie de persoonsgegevens niet rechtstreeks zijn verkregen, worden binnen een maand geïnformeerd.	<ul style="list-style-type: none"> Een logboek of register van berichten of communicaties met personen van wie de gegevens niet rechtstreeks zijn verkregen, waarbij de datum van verkrijging en de datum van communicatie zijn opgenomen.
	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.	<ul style="list-style-type: none"> Een link naar de privacyverklaring op de website of een screenshot van de pagina waarop de privacyverklaring zich bevindt. Voorbeelden van applicaties en formulieren waarin naar de privacyverklaring wordt verwezen.
	Er is cookiebeleid vastgelegd en dit voldoet aan wet- en regelgeving.	<ul style="list-style-type: none"> Een kopie van het cookiebeleid en/of richtlijn Eventueel een juridische beoordeling of goedkeuring van het cookiebeleid ten opzichte van de geldende wet- en regelgeving.
	De website informeert gebruikers over het cookiebeleid.	<ul style="list-style-type: none"> Screenshots van de website waarin het cookiebeleid wordt gepresenteerd of waar gebruikers expliciet worden geïnformeerd over cookies.
VWN4 - beheerst	Er wordt periodiek geëvalueerd of de procedures voor het informeren van betrokkenen adequaat zijn en worden nagekomen. Daar waar nodig worden aanpassingen doorgevoerd.	<ul style="list-style-type: none">
	De privacyverklaring is up-to-date en de inhoud wordt afgestemd op de specifieke context van applicaties en formulieren.	<ul style="list-style-type: none">
	Het cookiebeleid en de implementatie ervan worden periodiek geëvalueerd. Daar waar nodig worden aanpassingen doorgevoerd.	<ul style="list-style-type: none">
VWN5 - geoptimaliseerd	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.	<ul style="list-style-type: none">
	Applicaties en formulieren bieden uitgebreide uitleg over de verwerking van persoonsgegevens.	<ul style="list-style-type: none">
	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.	<ul style="list-style-type: none">

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	Het cookiebeleid en de implementatie ervan worden proactief getoetst aan de nieuwste inzichten en richtlijnen.	<ul style="list-style-type: none"><li data-bbox="1272 245 1283 261">•

RB.03 – Toestemming

Wat	Beschrijving	
Domein	Rechten van betrokkenen	
Categorie	Toestemming	
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • 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. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>De grondslag (toestemming) behoort te worden geregistreerd in het verwerkingsregister. Toestemmingsverklaringen moeten zodanig worden gedocumenteerd dat aangetoond kan worden dat betrokkene toestemming heeft verleend.</p> <p>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.</p> <p>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.</p> <p>Zorg dat de organisatie bij het vragen van toestemming voldoet aan de informatieplicht.</p>	
Toetsing	O&P	
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	<ul style="list-style-type: none"> • CFR02 • CFR03 	

Wat	Beschrijving
	<ul style="list-style-type: none"><li data-bbox="501 248 612 271">• CFR04

RB.03 – Bewijsmateriaal Toestemming

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Er zijn geen gestandaardiseerde processen voor de identificatie van verwerkingen die op toestemming zijn gebaseerd. Er is geen documentatie van toestemming Er is geen procedure om toestemming in te trekken.	•
VWN2 - herhaalbaar	De organisatie heeft een informeel proces om verwerkingen die op toestemming zijn gebaseerd te identificeren, maar dit proces wordt niet consequent gevolgd.	•
	De organisatie vraagt toestemming van betrokkenen, maar de toestemming is niet altijd vrij, geïnformeerd, specifiek en ondubbelzinnig.	•
	Toestemming wordt in een aantal gevallen gedocumenteerd, maar dit is nog niet consequent of volledig.	•
	Betrokkenen hebben de mogelijkheid om toestemming in te trekken, maar dit proces is niet altijd duidelijk of gemakkelijk.	•
VWN3 - bepaald	De organisatie heeft vastgesteld welke verwerkingen op toestemming zijn gebaseerd.	• Een overzicht of register van verwerkingsactiviteiten waaruit blijkt welke verwerkingen zijn gebaseerd op toestemming.
	Toestemming wordt correct gevraagd volgens de vereisten die zijn opgenomen in AVG artikel 4, grond 32, 33, 42, en 43.	• Voorbeelden van communicatiematerialen of formulieren die worden gebruikt om toestemming te vragen, inclusief duidelijke onderbouwing van hoe deze vraag in lijn is met de relevante AVG-artikelen.
	Toestemming wordt consequent en volledig gedocumenteerd.	<ul style="list-style-type: none"> • Voorbeelden van documentatie die de verleende toestemming aantoont, zoals formulieren, e-mails of digitale logs. • Een systeem of register dat consistent bijhoudt welke betrokkenen toestemming hebben gegeven, voor welke specifieke verwerkingen en wanneer.
	Betrokkenen kunnen hun toestemming gemakkelijk intrekken.	<ul style="list-style-type: none"> • Documentatie of richtlijnen over het proces van intrekking van toestemming. • Een overzicht of logboek van verzoeken tot intrekking van toestemming, met details over wanneer en hoe deze verzoeken zijn afgehandeld.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
		<ul style="list-style-type: none"> Voorbeelden van communicatiematerialen die betrokkenen informeren over hun recht om toestemming in te trekken.
VWN4 - beheerst	De organisatie evalueert periodiek haar processen om te bepalen welke verwerkingen op toestemming zijn gebaseerd.	<ul style="list-style-type: none">
	Er zijn periodieke beoordelingen en audits om ervoor te zorgen dat toestemming correct wordt gevraagd en gedocumenteerd.	<ul style="list-style-type: none">
	Het proces voor het intrekken van toestemming wordt periodiek geëvalueerd en indien nodig aangepast.	<ul style="list-style-type: none">
VWN5 - geoptimaliseerd	De organisatie heeft systemen en processen om te bepalen welke verwerkingen op toestemming zijn gebaseerd.	<ul style="list-style-type: none">
	Documentatie van toestemming wordt (automatisch) bijgewerkt en gevolgd via systemen.	<ul style="list-style-type: none">
	Betrokkenen kunnen hun toestemming gemakkelijk intrekken en intrekkingen worden tijdig verwerkt.	<ul style="list-style-type: none">

RB.04 - Geautomatiseerde besluitvorming

Wat	Beschrijving
Domein	Rechten van betrokkenen
Categorie	Geautomatiseerde individuele besluitvorming waaronder profilering (Geautomatiseerde besluitvorming en/of profilering)
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> risico's voor de rechten en vrijheden van personen door verkeerde besluitvorming omtrent de bescherming van persoonsgegevens. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> 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	<p>Als geautomatiseerde besluitvorming en/of profilering wordt toegepast, wordt geadviseerd om een procedure te implementeren waarin is opgenomen:</p> <ul style="list-style-type: none"> 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. <p>Beheersing van geautomatiseerde besluitvorming is essentieel (maatschappelijk onder hoge aandacht). Zie voor de VWN4.2 genoemde AI-act onder andere:</p> <ul style="list-style-type: none"> EURLEX Europees Parlement AP inzet AI Act
Toetsing	O&P
AVG-UAVG	AVG 22 UAVG 40
ISO 27701:2019	7.4
VNG 3.0	4.4
Norea PCF	<ul style="list-style-type: none"> DAR01 PIA01

RB.04 – Bewijsmateriaal Geautomatiseerde besluitvorming

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Er is niet of onvoldoende bekend of er geautomatiseerde individuele besluitvorming en/of profilering binnen de organisatie plaatsvindt. Betrokkenen worden niet of nauwelijks geïnformeerd over geautomatiseerde individuele besluitvorming en/of profilering.	•
VWN2 - herhaalbaar	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.	•
	DPIA's worden niet consequent voor elke nieuwe of gewijzigde geautomatiseerde individuele besluitvorming en/of profilering uitgevoerd.	•
	Betrokkenen worden op ad hoc basis geïnformeerd over deze vorm van besluitvorming.	•
	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.	•
VWN3 - bepaald	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.	• Een algoritmeregister of gelijkwaardige documentatie die een overzicht biedt van alle algoritmes en processen die worden gebruikt voor geautomatiseerde besluitvorming en/of profilering.
	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.	<ul style="list-style-type: none"> • Gedocumenteerde procedures voor geautomatiseerde besluitvorming en/of profilering. • Communicatiematerialen, waaronder e-mails of brieven, die aan betrokkenen worden gestuurd om hen te informeren over hun rechten met betrekking tot geautomatiseerde besluitvorming en profilering. • Indien van toepassing, een overzicht van gevallen waarin betrokkenen hun standpunt hebben kenbaar gemaakt of besluiten hebben aangevochten, met details over de uitkomst en afhandeling.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	Betrokkenen worden geïnformeerd over geautomatiseerde besluitvorming en/of profilering op een wijze die in overeenstemming is met de informatieplicht.	<ul style="list-style-type: none"> Voorbeelden van mededelingen, zoals privacy-verklaringen of notificaties, die specifiek ingaan op geautomatiseerde besluitvorming en profilering. Onderbouwing van hoe de verstrekte informatie voldoet aan de informatieplicht.
	Er wordt een DPIA uitgevoerd voor elke nieuwe geautomatiseerde besluitvorming en/of profilering.	<ul style="list-style-type: none"> Gedocumenteerde resultaten van uitgevoerde DPIA's voor geautomatiseerde besluitvorming en/of profilering.
VWN4 - beheerst	Geautomatiseerde besluiten en/of profilering, worden periodiek geëvalueerd.	<ul style="list-style-type: none">
	Periodiek worden gerelateerde DPIA's geëvalueerd. Daar waar nodig worden de privacy waarborgen verbeterd.	<ul style="list-style-type: none">
	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.	<ul style="list-style-type: none">
	De organisatie communiceert proactief informatie over deze vorm van besluitvorming aan betrokkenen.	<ul style="list-style-type: none">
VWN5 - geoptimaliseerd	Er is een (interne) tool waarmee geautomatiseerde besluiten en/of profilering, eenvoudig kunnen worden bijgehouden en geëvalueerd op juistheid.	<ul style="list-style-type: none">
	De organisatie voorziet belanghebbenden van actuele informatie op basis waarvan automatische besluitvorming plaatsvindt.	<ul style="list-style-type: none">
	De organisatie past continu DPIA's toe op geautomatiseerde besluitvorming en/of profilering, waarbij de resultaten worden gebruikt om processen te verbeteren.	<ul style="list-style-type: none">

Samenwerking

SW.01 - Externe AVG-rollen

Wat	Beschrijving
Domein	Samenwerking
Categorie	AVG-rollen
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen door een gebrek aan verantwoordelijkheid en controle. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>Denk bij betrokken partijen aan de verwerking van persoonsgegevens door externe partijen in zowel onderwijs, onderzoek als bedrijfsvoering, maar ook in samenwerkingsverbanden, (data-)uitwisselingen.</p> <p>De organisatie is niet in alle gevallen (alleen) verwerkingsverantwoordelijke. In dat geval kan sprake zijn van gezamenlijke verantwoordelijkheid.</p> <p>Soms wordt verantwoordelijkheid ook overgedragen. Denk bijvoorbeeld aan gegevens die naar de belastingdienst gaan.</p> <p>Daarnaast eigen en 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.</p>
Toetsing	0
AVG-UAVG	AVG 26 AVG 28
ISO 27701:2019	7.2
VNG 3.0	5.
Norea PCF	<ul style="list-style-type: none"> • RRE01 • RRE03

SW.01 – Bewijsmateriaal Externe AVG-rollen

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	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. Voorafgaand aan een verwerking voert de organisatie geen beoordeling uit om te bepalen of een externe optreedt als gegevensverwerker, gezamenlijke verwerkingsverantwoordelijke of zelfstandige verwerkingsverantwoordelijke. Er worden geen of nauwelijks afspraken gemaakt met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken	•
VWN2 - herhaalbaar	Medewerkers hebben beperkt bewustzijn van het belang van het onderscheiden van AVG-rollen.	•
	De organisatie heeft de AVG-rollen van de organisatie en die van externe partijen deels inzichtelijk gemaakt, maar dit is gefragmenteerd en inconsistent.	•
	Er wordt incidenteel een beoordeling uitgevoerd om te bepalen of de externe partij optreedt als gegevensverwerker, gezamenlijke verwerkingsverantwoordelijke, of zelfstandige verwerkingsverantwoordelijke, maar dit gebeurt niet systematisch en is sterk afhankelijk van individuen of afdelingen.	•
	Er worden in sommige gevallen afspraken gemaakt met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken, maar dit is niet uniform.	•
	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	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.	<ul style="list-style-type: none"> • Register of overzicht waarin de AVG-rollen van alle betrokken partijen zijn gedefinieerd. • Rolverdeling staat duidelijk omschreven in contracten of samenwerkingsovereenkomsten, dan wel daarbij horende bijlagen; zoals een gegevensuitwisselings- of gezamenlijke verantwoordelijkheidsovereenkomst

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	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.	<ul style="list-style-type: none"> • Gedocumenteerde procedures of checklists voor het evalueren van externe partijen. Bijvoorbeeld Pre-DPIA of DPIA-Check. • Voorbeelden van uitgevoerde evaluaties of assessments voor recente projecten.
	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.	<ul style="list-style-type: none"> • Steekproef van de overeenkomsten met derde partijen waaruit blijkt dat de vereiste AVG-bepalingen zijn opgenomen. • Een communicatiekanaal of systeem voor het melden van wijzigingen in de verwerkingsactiviteiten. • Controles zijn onderdeel van Leveranciers- en contractmanagement.
	Het beheer van overeenkomsten met verwerkers, zelfstandig verwerkingsverantwoordelijken en gezamenlijke verwerkingsverantwoordelijken is adequaat belegd binnen de organisatie.	<ul style="list-style-type: none"> • Een gestructureerd archief of digitaal systeem waarin overeenkomsten worden bewaard. • Taken- en verantwoordelijkheidsoverzicht waaruit blijkt welke functionaris of afdeling verantwoordelijk is voor het beheer van deze overeenkomsten.
VWN4 - beheerst	AVG-rollen van externe partijen worden periodiek geëvalueerd. Indien noodzakelijk worden beleid en procedures aangepast.	<ul style="list-style-type: none"> •
	Naleving van de afspraken die zijn gemaakt met verwerkers en gezamenlijke verwerkingsverantwoordelijken wordt periodiek getoetst of geaudit.	<ul style="list-style-type: none"> •
	De afspraken met verwerkers, gezamenlijke verwerkingsverantwoordelijken en eventueel zelfstandig verwerkingsverantwoordelijken worden periodiek geëvalueerd en aangepast indien nodig.	<ul style="list-style-type: none"> •
	Het beheer en evaluatie van overeenkomsten met verwerkers, zelfstandig verwerkingsverantwoordelijken en gezamenlijke verwerkingsverantwoordelijken is goed georganiseerd en wordt periodiek geëvalueerd en waar nodig aangepast.	<ul style="list-style-type: none"> •
	Training en bewustwording over AVG-rollen zijn geïntegreerd in de processen en procedures van de organisatie.	<ul style="list-style-type: none"> •
VWN5 - geoptimaliseerd	Er is een eenvoudig en toegankelijk tool/systeem dat een overzicht/rapportages biedt van de AVG-rollen van externe partijen.	

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	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.	

SW.02 - Eenmalige verstrekkingen

Wat	Beschrijving
Domein	Samenwerking
Categorie	Toetsing gegevensverstrekking aan derden
Beschrijving risico	<p>Het ontbreken van een uniform toetsingskader voor gegevensverstrekking aan derden en/of een systematische beoordeling daarvan waardoor gegevens mogelijk onrechtmatig en/of ongeautoriseerd aan derden worden verstrekt. Dit kan leiden tot:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen door onrechtmatige gegevensverstrekking. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>Gegevensverstrekking aan derden dient gedocumenteerd te worden. Ten minste de volgende informatie dient te worden vastgelegd:</p> <ul style="list-style-type: none"> • gegevens over de ontvanger. • de categorieën van persoonsgegevens. • de doeleinden. • de rechtsgrond voor verstrekking.
Toetsing	O&P
AVG-UAVG	AVG 5 AVG 6
ISO 27701:2019	7.5 8.5
VNG 3.0	5.2
Norea PCF	<ul style="list-style-type: none"> • TPD01 • UKI01

SW.02 – Bewijsmateriaal eenmalige verstrekkingen

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	De organisatie heeft geen eenduidige, gestandaardiseerde procedure vastgesteld voor de toetsing van gegevensverstrekking aan derden. 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	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.	•
	Een coherente, organisatiebrede procedure ontbreekt, wat leidt tot inconsistenties en variatie in de kwaliteit van de toetsingen.	•
	Relevante medewerkers (zoals inkoop, juridische afdeling, onderzoekers) hebben beperkt bewustzijn van het belang van het toetsen van de gegevensverstrekking aan externe partijen.	•
VWN3 - bepaald	De organisatie heeft een uniform, organisatiebreed kader geïmplementeerd voor het toetsen van gegevensverstrekking aan externe partijen, dat consequent wordt toegepast in de gehele organisatie.	<ul style="list-style-type: none"> • Een kopie van het organisatiebrede kader voor het toetsen van gegevensverstrekking aan derden. • Documentatie of logs die aantonen dat dit kader consequent wordt toegepast bij besluitvormingsprocessen betreffende gegevensverstrekking.
	De organisatie heeft het kader met daarin zowel het toetsingsproces als de besluitvorming daaromtrent gedocumenteerd.	<ul style="list-style-type: none"> • Documenten die het toetsingsproces en de besluitvorming omtrent gegevensverstrekking beschrijven. • Voorbeelden van eerdere toetsingen, met inbegrip van de uitkomst en de redenering achter de beslissing.
	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.	<ul style="list-style-type: none"> • Trainingsmateriaal, presentaties of beleid over de toetsing van gegevensverstrekking.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	Medewerkers weten wie ze kunnen benaderen om te toetsen of een eenmalige gegevensverstrekking in overeenstemming is met de wet- en regelgeving.	<ul style="list-style-type: none"> • Een duidelijk gedefinieerde contactlijst of procedure die aangeeft welke functionarissen of afdelingen moeten worden geraadpleegd voor toetsingsverzoeken. • Communicatie of memo's naar medewerkers die duidelijk maken hoe en wie ze moeten benaderen voor toetsingsverzoeken.
VWN4 - beheerst	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.	<ul style="list-style-type: none"> •
	De toetsingsprocedures worden periodiek geëvalueerd en indien nodig aangepast.	<ul style="list-style-type: none"> •
	Training en bewustmaking over gegevensverstrekking aan externe partijen zijn geïntegreerd in de reguliere bedrijfsprocessen en -procedures.	<ul style="list-style-type: none"> •
	Er is een gemakkelijk vindbaar overzicht van alle gegevensverstrekkingen aan externe partijen beschikbaar, bijvoorbeeld via een specifieke interne tool of systeem.	<ul style="list-style-type: none"> •
VWN5 - geoptimaliseerd	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.	<ul style="list-style-type: none"> •

SW.03 - Doorgifte buiten EER

Wat	Beschrijving	
Domein	Samenwerking	
Categorie	Doorgifte buiten de EER	
Beschrijving risico	<p>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.</p> <p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen door onrechtmatige verwerking en/of onvoldoende bescherming van persoonsgegevens. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p>	
Toetsing	O&P	
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	<ul style="list-style-type: none"> • PPO05 • DTR01 • DTR02 	

SW.03 – Bewijsmateriaal buiten EER

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Binnen de organisatie is er onvoldoende bekendheid over de procedures die moeten worden gevolgd bij het overdragen van gegevens buiten de EER. De organisatie heeft geen (duidelijk) inzicht in de landen waaraan persoonsgegevens worden doorgegeven. Periodieke toetsing van de naleving van wet- en regelgeving met betrekking tot de doorgifte van persoonsgegevens aan derde landen (buiten de EER) ontbreekt.	<ul style="list-style-type: none"> •
VWN2 - herhaalbaar	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.	<ul style="list-style-type: none"> •
	Er is geen gestandaardiseerde procedure voor het documenteren van landen waaraan persoonsgegevens worden doorgegeven wat het risico op inconsistenties en fouten verhoogt.	<ul style="list-style-type: none"> •
VWN3 - bepaald	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.	<ul style="list-style-type: none"> • Documentatie van recent uitgevoerde toetsingen voor doorgiftes naar landen buiten de EER. • Een procedure of richtlijn voor het uitvoeren van de toetsing op passend beschermingsniveau.
	Er is een duidelijk en consistent proces voor het documenteren van landen waaraan persoonsgegevens worden doorgegeven.	<ul style="list-style-type: none"> • Een overzicht of database met landen waaraan persoonsgegevens worden doorgegeven, inclusief de details van de gegevensverwerking en ontvangende entiteiten. (Opgenomen in het Register van Verwerkingsactiviteiten en duidelijk aangegeven in de Verwerkingsovereenkomst(-en). • Procedure of handleiding voor het documenteren van doorgiftes naar landen buiten de EER.
	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.	<ul style="list-style-type: none"> • Documentatie van recente herbeoordelingen van bestaande doorgiftes naar landen buiten de EER. • Een beleidsdocument of handleiding die de frequentie en methodiek van deze periodieke herbeoordelingen beschrijft.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
		<ul style="list-style-type: none"> • Toetsing op basis van Verwerkingsovereenkomsten • Communicatie of training gericht aan relevante medewerkers over dit herbeoordelingsproces.
VWN4 - beheerst	De organisatie evalueert periodiek de doorgiften buiten de EER en past indien nodig de (toets-)processen aan.	<ul style="list-style-type: none"> •
	De periodieke evaluaties worden ondersteund door bewustwordingscampagnes en/of training om de kennis en het bewustzijn over doorgiften buiten de EER binnen de organisatie te verhogen.	<ul style="list-style-type: none"> •
VWN5 - geoptimaliseerd	De organisatie heeft een tool geïmplementeerd om inzicht te krijgen in gegevensverstrekkingen waaronder doorgiften naar derde landen, wat ook het proces van het monitoren en periodiek evalueren van de gegevensverstrekkingen vergemakkelijkt.	<ul style="list-style-type: none"> •
	De organisatie is in staat om te reageren op veranderingen in de omstandigheden of wet- en regelgeving over doorgifte buiten de EER.	<ul style="list-style-type: none"> •

Gegevensbescherming

GB.01 - Datalekken behandelen

Wat	Beschrijving
Domein	Gegevensbescherming
Categorie	Datalekken detectie, classificatie en afhandeling
Beschrijving risico	<p>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 inadequaate behaalde 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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> risico's voor de rechten en vrijheden van personen door het niet tijdig detecteren of afhandelen van datalekken. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> 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	De organisatie heeft een proces vastgesteld en gedocumenteerd voor de detectie, classificatie en be-/afhandeling van datalekken.
Toelichting	<p>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.</p> <p>Het datalekkenregister bevat ten minste:</p> <ul style="list-style-type: none"> 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
AVG-UAVG	VG 4 sub 12, AVG 33 AVG 34
ISO 27701:2019	6.3.1.1
VNG 3.0	6.5
Norea PCF	<ul style="list-style-type: none"> PBI01 PBI03 PBI04 PBI05 <ul style="list-style-type: none"> PBI06 PBI07 PBI08 PBI09

GB.01 – Bewijsmateriaal Datalekken behandelen

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Er ontbreekt een (centraal) meldpunt voor privacyincidenten dat toegankelijk is voor alle medewerkers, onderwijsdeelnemers en overige betrokkenen. Er is geen gestructureerd proces voor het detecteren, classificeren en afhandelen van datalekken. Er is niet duidelijk wanneer een (beveiligings)incident een datalek is. Incidenten worden afgehandeld op ad hoc basis, en worden niet geëvalueerd. Er is geen datalekkenregister.	•
VWN2 - herhaalbaar	Er is geen makkelijk vindbaar meldpunt voor privacyincidenten voor alle medewerkers, onderwijsdeelnemers en overige betrokkenen, en/of het is niet gemakkelijk toegankelijk.	•
	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.	•
	Classificatie van incidenten waarbij persoonsgegevens zijn betrokken op impact/risico voor betrokkenen is afhankelijk van de individuele medewerker die de classificatie uitvoert.	•
	Evaluatie van incidenten waarbij persoonsgegevens zijn betrokken wordt ad hoc uitgevoerd.	•
	Het datalekkenregister wordt ad hoc ingevuld.	•
VWN3 - bepaald	Er is een makkelijk vindbaar en gemakkelijk toegankelijk meldpunt voor privacyincidenten.	<ul style="list-style-type: none"> • Een link of referentie naar het online meldpunt voor privacyincidenten. • Documentatie of communicatiemateriaal waarin medewerkers worden geïnformeerd over dit meldpunt.
	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,	<ul style="list-style-type: none"> • Een gedetailleerde procedure of beleidsdocument waarin het proces voor datalekken wordt beschreven, inclusief alle genoemde subpunten. • Training- of bewustwordingsmateriaal dat specifiek gericht is op dit proces en aan relevante medewerkers wordt verstrekt.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	<p>een risicobeoordeling c.q. afwegingskader waar het al dan niet melden van een datalek onderdeel van is respons- en escalatie, beheersing, herstel, evaluatie</p>	
	<p>Incidenten worden systematisch geëvalueerd om verbeteringen te identificeren.</p>	<ul style="list-style-type: none"> • Documentatie van recente post-incident evaluaties, inclusief aanbevelingen voor verbetering. • Een vastgelegde procedure of methode voor het uitvoeren van deze evaluaties.
	<p>De resultaten van de evaluaties worden met het management gedeeld.</p>	<ul style="list-style-type: none"> • Notulen van vergaderingen of besprekingen waarin de resultaten van incidentevaluaties zijn besproken. • E-mails of andere communicatiemiddelen waarin deze resultaten aan het management worden gemeld.
	<p>Er is een datalekkenregister dat regelmatig wordt bijgewerkt. Het register bevat alle (gemelde) datalekken.</p>	<ul style="list-style-type: none"> • Schermprint van het register
VWN4 - beheerst	<p>Het proces voor het detecteren, classificeren en afhandelen van datalekken wordt periodiek geëvalueerd om de effectiviteit ervan te waarborgen en indien nodig aangepast.</p>	<ul style="list-style-type: none"> •
	<p>De vindbaarheid van het privacy meldpunt wordt periodiek geëvalueerd.</p>	<ul style="list-style-type: none"> •
	<p>Het datalekkenregister wordt regelmatig geëvalueerd.</p>	<ul style="list-style-type: none"> •
VWN5 - geoptimaliseerd	<p>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. Deze resultaten van de evaluatie van datalekken worden gedeeld met het management en indien van toepassing binnen de gehele organisatie. De organisatie gebruikt de informatie uit het register proactief om toekomstige datalekken te voorkomen en de algehele privacy te verbeteren.</p>	<ul style="list-style-type: none"> •

GB.02 - Datalekken communiceren

Wat	Beschrijving
Domein	Gegevensbescherming
Categorie	Melding van datalekken aan AP en betrokkenen
Beschrijving risico	<p>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.</p> <p>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.</p> <p>Het ontbreken van duidelijke verantwoordelijkheden en tijdslijnen kan het proces vertragen en de impact onnodig vergroten. Dit kan leiden tot:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen door het niet tijdig mededelen van inbreuk op de persoonsgegevens met hoog risico voor betrokkenen. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, en er een risico is voor betrokkene, meldt de verwerkingsverantwoordelijke dit aan de Autoriteit Persoonsgegevens.</p> <p>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).</p> <p>In dit toetsingskader noemen we beiden "melden".</p> <p>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.</p>
Toetsing	O
AVG-UAVG	AVG 4 sub 12, AVG 33 AVG 34
ISO 27701:2019	6.13.1.1
VNG 3.0	6.5
Norea PCF	<ul style="list-style-type: none"> • PBI01 • PBI03 • PBI04 • PBI05 • PBI06 • PBI07 • PBI08 • PBI09

GB.02 – Bewijsmateriaal Datalekken communiceren

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	Er is geen proces voor melden van datalekken aan de AP en betrokkenen.	•
	Er is geen duidelijkheid over wie verantwoordelijk is voor het melden van een datalek aan de AP en betrokkenen.	•
	Er zijn geen vastgestelde tijdslijnen voor het melden van een datalek aan de AP en betrokkenen.	•
	Er is geen woordvoerder voor de communicatie over (mogelijke) datalekken met betrokkenen en/of media.	•
VWN2 - herhaalbaar	Er bestaat een Informeel proces voor het melden van datalekken aan de AP en betrokkenen, maar de implementatie en naleving zijn inconsistent.	•
	Verantwoordelijkheden voor het afhandelen en communiceren van datalekken zijn gedefinieerd, maar zijn niet altijd duidelijk voor alle betrokken partijen.	•
	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.	•
VWN3 - bepaald	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.	<ul style="list-style-type: none"> • Een beleidsdocument of procedure waarin het proces voor melding van datalekken aan de AP en betrokkenen is beschreven, inclusief de communicatierichtlijnen, verantwoordelijkheden, documentatievereisten en tijdslijnen. • Training- of bewustwordingsmateriaal gericht op dit proces dat aan relevante medewerkers wordt verstrekt.
	Er is een crisiscommunicatieplan voor datalekken met hoge impact.	<ul style="list-style-type: none"> • Een exemplaar van het crisiscommunicatieplan specifiek voor datalekken. • Verslagen of notulen van oefensessies of simulaties gebaseerd op het crisiscommunicatieplan.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	Het proces wordt consistent nageleefd.	<ul style="list-style-type: none"> • Steekproefsgewijze checks of audits die bevestigen dat de procedures worden gevolgd bij daadwerkelijke datalekken.
VWN4 - beheerst	Het proces voor het melden van datalekken aan de AP en betrokkenen is volledig geïntegreerd in de organisatie, met consistente uitvoering en naleving.	<ul style="list-style-type: none"> •
	Het proces voor het melden van datalekken aan de AP en betrokkenen wordt periodiek geëvalueerd en, indien nodig, aangepast.	<ul style="list-style-type: none"> •
	Het crisiscommunicatieplan voor datalekken met hoge impact wordt periodiek geoefend, en indien nodig, herzien.	<ul style="list-style-type: none"> •
VWN5 - geoptimaliseerd	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.	<ul style="list-style-type: none"> •
	Het management wordt systematisch geïnformeerd over alle datalekken en genomen maatregelen.	<ul style="list-style-type: none"> •
	Er bestaat een hiërarchie (escalatieregels) voor escalatie naar de juiste managementniveaus.	<ul style="list-style-type: none"> •

GB.03 – Informatiebeveiliging

Wat	Beschrijving
Domein	Gegevensbescherming
Categorie	Informatieveiligheid
Beschrijving risico	<p>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:</p> <p>Voor betrokkenen:</p> <ul style="list-style-type: none"> • risico's voor de rechten en vrijheden van personen door het ongewenst openbaar worden, manipulatie of niet beschikbaar zijn van gegevens. <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>Adequate informatiebeveiliging om persoonsgegevens te beschermen. De relevante IB-maatregelen die hierbij passen:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p> <p>Artikel 32 lid 1 stelt dat de beveiliging onder meer het volgende moet omvatten:</p> <ul style="list-style-type: none"> • de pseudonimisering en versleuteling van persoonsgegevens; • het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid de veerkracht van de verwerkingsystemen 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;

Wat	Beschrijving
	<ul style="list-style-type: none"><li data-bbox="504 248 1401 331">• 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.

GB.03 – Bewijsmateriaal Informatiebeveiliging

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
<p>Beheerdoelstelling</p>	<p>Adequate informatiebeveiliging om persoonsgegevens te beschermen. De relevante IB-maatregelen die hierbij passen:</p> <ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Bij dit statement kan ervoor gekozen worden het resultaat van de informatiebeveiliging benchmark over te nemen. Ook kan ervoor gekozen worden om middels het tabblad informatiebeveiliging de daarin zittende (13) statements in te vullen en dit resultaat bij dit statement in te voeren.
<p>Toelichting</p>	<p>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:</p> <ul style="list-style-type: none"> • 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; 	<ul style="list-style-type: none"> •

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
	<ul style="list-style-type: none">• 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	<p>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.</p> <p>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:</p> <p>Voor de organisatie:</p> <ul style="list-style-type: none"> • 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	<p>Geadviseerd wordt om in het periodieke privacy verslag voor interne stakeholders ten minste de volgende onderwerpen op te nemen:</p> <ul style="list-style-type: none"> • globaal overzicht verwerkingsregister. • uitgevoerde DPIA's. • verslag over datalekken. • verzoeken rechten van betrokkenen. • resultaten van het SURFaudit Toetsingskader Privacy benchmark. • verbeterplan. <p>Voor verantwoording aan externe stakeholders kan worden gedacht aan:</p> <ul style="list-style-type: none"> • informatie voor onderwijsdeelnemers. • een alinea/paragraaf in het algemene jaarverslag van de organisatie, gebaseerd op het uitgebreidere interne privacy verslag. <p>N.B. Dit privacyverslag betreft niet het verslag dat de FG vanuit zijn/haar toezichthoudersrol opstelt</p>
Toetsing	O&P
AVG-UAVG	AVG5 lid 2 AVG 39
ISO 27701:2019	-
VNG 3.0	7.3
Norea PCF	

VW.01 – Bewijsmateriaal Rapportage

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
VWN1 - ad hoc	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.	•
	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	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.	•
	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	Er wordt een gestructureerd en gedocumenteerd proces gevolgd voor het opstellen van een periodiek verslag waarin zowel interne (inclusief het bestuur) als externe stakeholders 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.	<ul style="list-style-type: none"> • Een officieel beleidsdocument of procedure waarin het proces voor het opstellen en publiceren van het verslag is beschreven. • Opgenomen als onderdeel van de planning & controlcyclus en bijbehorende jaarrapportages. • Bewijs van raadpleging, advies of andere aantoonbare betrokkenheid van de FG bij het opstellen van het verslag, zoals e-mailcorrespondentie of vergadernotulen. • Bewijs waaruit blijkt dat het opgestelde verslag wordt gedeeld met het bestuur en externe belanghebbenden zoals Raad van Toezicht, Koepels, en opgenomen in het jaarverslag.
	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.	<ul style="list-style-type: none"> • Een overzicht, rapportage of dashboard waarin gegevens uit verschillende afdelingen samenkomen over de omgang met persoonsgegevens of de status van de implementatie van privacymaatregelen.

Volwassenheidsniveau	Bijbehorende aanpak in de organisatie	Wat heb je nodig als bewijsmateriaal?
		<ul style="list-style-type: none"> • Documentatie over het proces van het verzamelen van deze gegevens van verschillende afdelingen.
	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.	<ul style="list-style-type: none"> • Voorbeelden van eerdere organisatieverslagen, controles of audits waarin deze aspecten worden behandeld zoals het verwerkingsregister, DPIA's, datalekken, enz. • Een overzicht of planning van de frequentie waarmee deze verslagen worden opgesteld en gepubliceerd.
	De verantwoordelijkheden voor het opstellen en verspreiden van dit verslag zijn duidelijk aantoonbaar toegewezen.	<ul style="list-style-type: none"> • Een organisatieschema of RACI-matrix waarin de verantwoordelijkheden voor rapportage zijn vastgelegd. • Bewijs van communicatie of toewijzing van deze verantwoordelijkheden, zoals e-mailcorrespondentie, taaktoewijzing
VWN4 - beheerst	De inhoudelijke elementen van de rapportage en het rapportageproces worden periodiek geëvalueerd en indien nodig aangepast.	<ul style="list-style-type: none"> •
	Op basis van rapportage worden verbeterplannen opgesteld en wordt gerapporteerd over de uitvoering hiervan.	<ul style="list-style-type: none"> •
VWN5 - geoptimaliseerd	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.	<ul style="list-style-type: none"> •
	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.	<ul style="list-style-type: none"> •
	Er wordt gebruik gemaakt van tools en methodes om informatie op een toegankelijke en begrijpelijke manier te presenteren, bijvoorbeeld via animaties.	<ul style="list-style-type: none"> •
	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.	

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

Niveau	Titel	Beschrijving
1	Ad hoc	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • (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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none">• 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 volgende 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.