Handreiking auditmethodiek Toetsingskader Privacy

Auditmethodiek voor benchmark en self-assessment bij het gebruik van het SURF Toetsingskader Privacy



Colofon

Dit document is bedoeld als praktische handreiking voor de auditmethodiek bij het gebruik van het SURF Toetsingskader Privacy. Het is te gebruiken als hulpmiddel bij audits (self-assessment) en de sector-benchmark.

Bestemd voor

Dit document is specifiek bestemd voor privacyteams en hun collega's (bijvoorbeeld het interne auditteam) die zich bezighouden met de implementatie van het SURF Toetsingskader Privacy en controle daarop.

Samenstelling en beheer

Dit document is tot stand gekomen met vertegenwoordigers uit de onderwijssector (werkgroep) en de SURF-dienst 'SURFaudit' en adviseur Erik van den Beld. Speciale dank gaat uit naar de werkgroepleden.

Licentie

Dit document is verstrekt onder de creative commons-licentie **CC BY** 4.0 International (naamsvermelding). SURF aanvaardt geen aansprakelijkheid voor enig gebruik/toepassing van dit document.

Versiebeheer

Versie	Door	Datum	Toelichting/wijziging
1.0	Sectorwerkgroep en SURF	November 2024	Initieel document
1.1	SURF (PEC)	25-09-2026	Focus op auditinfo, dubbele informatie van het toetsingskader verwijderd + verwijzingen aangebracht

Inhoudsopgave

Colofon 2

1 Inleiding 4

1.1 Doel en ambitie 4
1.2 Uitgangspunten 4
1.3 De dienst SURFaudit 5
1.4 Werking van de volwassenheidsniveaus 5
1.4.1 vijf volwassenheidniveau 5
1.4.2 Volwassenheidsniveaus 1 en 2 5
1.4.3 Het belang en betekenis van niveau 3 5
1.4.4 De betekenis van niveau 4 6
1.4.5 Het streven naar niveau 5 6
1.5 Overwegingen volwassenheidsniveaus privacykader 6
1.6 Rapportage benchmark SURFaudit 7

2 Scope voor privacyaudit bepalen 8

2.1 Inleiding 8
2.2 Processen 8
2.2.1 Verwerking persoonsgegevens binnen onderwijsprocessen 8
2.2.2 Verwerking persoonsgegevens binnen onderzoek 9
2.2.3 Verwerking persoonsgegevens binnen de processen van bedrijfsvoering 9
2.3 Risico-gebaseerde scopebepaling 9
2.3.1 Aanpak voor risico-gebaseerde scopebepaling 9
2.4 Overige aanbevelingen voor scopebepaling: 11

3 Scope benchmark SURF Toetsingskader Privacy 11

3.1 Samenvatting scope 12

4 Audittechnieken 13

4.1 Onderzoek 13
4.2 Observatie 13
4.3 Inspectie 13
4.4 Herhaling (heruitvoering) 13

5 Auditmethodiek – stappenplan 14

5.1 Stap 1 – Voorbereiden 14
5.2 Stap 2 – Type audit 14
5.3 Stap 3 – Uitvoeren 14
5.4 Stap 4 – Rapporteren 15
5.5 Stap 5 – Borging 15

Bijlage 1 - Voorbeeldplanning (bij deelname aan benchmark) 16

Bijlage 2 - Aandachtspunten bij nazorg 17

Bijlage 3 - Definities 18

1 Inleiding

Het SURF Toetsingskader Privacy (ook: 'privacykader') biedt organisaties een 'meetinstrument' om inzicht te krijgen in de eigen volwassenheid in het naleven van de AVG. Daarmee levert het voor organisaties input voor verdere verbetering van de bescherming van persoonsgegevens.

De in dit document beschreven auditmethodiek kun je gebruiken hulpmiddel om beheersmaatregelen uit het privacykader te toetsen op implementatie en naleving. De auditmethodiek geeft je een gestructureerde benadering voor audits en zelfevaluaties.

Hiermee kun je:
- een ambitie formuleren (volwassenheidsniveau) en/of groeidoelen en bijbehorende acties bepalen;
- de resultaten integreren in de jaarplannen van de organisatie en/of onderdelen daarvan;
- de eigen resultaten via de benchmark van SURFaudit vergelijken met de rest van de sector;
- kennis & ervaring wisselen of een peerreview uitvoeren.

Hiermee zorgt de auditmethodiek voor een brug tussen ambitie/beleid en praktijk.

1.1 Doel en ambitie

De handreiking biedt een eenduidige auditmethodiek om organisaties te ondersteunen bij audits en zelfevaluaties en maakt onderlinge vergelijking in de sector mogelijk. Deze auditmethodiek helpt om gestructureerd de effectiviteit van de bescherming van rechten en vrijheden van personen en de naleving van de AVG/UAVG te beoordelen volgens het SURF Toetsingskader Privacy. Met deze auditvorm kunnen organisaties controleren waar ze staan qua bescherming van persoonsgegevens, waar verbeterpunten liggen en hoe ze zich verhouden tot hun sectorgenoten.

1.2 Uitgangspunten

- Een gemeenschappelijke sectorbrede aanpak op basis van het SURF Toetsingskader Privacy.
- Een eenduidige aanpak waarbij scope en diepgang van de audit bij alle organisaties (bij benadering) hetzelfde zijn, voor goed vergelijkbare resultaten.
- Het privacykader is bruikbaar voor self-assessments, interne audits, peerreviews en externe audits.
- SURF organiseert jaarlijks een benchmark met als deadline 31 januari voor het indienen van de resultaten. Openstelling vanaf de 1e week van oktober.
- Organisaties voeren bij voorkeur tweejaarlijks afwisselend een self-assessment of een (interne/externe) audit uit.
- De resultaten die een organisatie bij SURF indient voor de benchmark zijn niet ouder dan een jaar. Dat betekent dat de resultaten bijgewerkt moeten worden naar de actuele stand van zaken als een audit meer dan een jaar daarvoor is uitgevoerd.
- De audit omvat de procesmatige, technische en organisatorische beheersmaatregelen.

1.3 De dienst SURFaudit

SURFaudit is een SURF-dienst die o.a. voorziet in ondersteuning bij audits, kennisproducten en applicaties op het gebied van Governance, Compliance en Risk. Als onderdeel van SURFaudit, wordt jaarlijks een benchmark georganiseerd. Het programma bestaat uit een cyclus van self-assessments of audits en benchmarks op het vlak van Informatiebeveiliging (IB) en Privacy (P).

1.4 Werking van de volwassenheidsniveaus

1.4.1 Vijf volwassenheidsniveaus

Het privacykader hanteert vijf volwassenheidsniveaus. In deze handreiking beschrijven we de algemene werking van volwassenheidsniveaus. In de bijlage van het privacykader vind je specifieke uitleg over de privacycriteria.

Elk volwassenheidsniveau bouwt voort op het vorige, met uitzondering van de maatregelen op niveaus 1 en 2. Dat wil zeggen dat om niveau 4 van een statement te bereiken, je eerst moet voldoen aan alle maatregelen van niveau 3, en zo verder.

In de sector Onderwijs & Onderzoek streven we volwassenheidsniveau 3 na.
Op dit niveau zijn beheersmaatregelen gedocumenteerd en worden ze op een gestructureerde en formele manier uitgevoerd. De uitvoering van de maatregelen is aantoonbaar en er is sprake van periodieke controle of de werkwijze nog actueel is.

1.4.2 Volwassenheidsniveaus 1 en 2

- Niveau 1 is het instapniveau, waarbij slechts minimale (ad hoc) maatregelen worden genomen. Men is onbewust onbekwaam.
- Niveau 2 is een overgangsniveau waarbij maatregelen herhaal zijn. Het helpt organisaties te begrijpen welke stappen nodig zijn om van niveau 1 naar niveau 3 te groeien. Men is bewust onbekwaam.

1.4.3 Het belang en betekenis van niveau 3

- Niveau 3 geeft aan dat de basismaatregelen voor alle relevante onderdelen adequaat zijn geïmplementeerd en dat dit aantoonbaar is. Men is bewust bekwaam.
- Dit geldt per statement en niet op het gemiddelde.
- De basis voor een verbetercyclus is aanwezig om te controleren of de werkwijze nog aansluit bij de praktijk.

1.4.4 De betekenis van niveau 4

- Voor niveau 4 is over het algemeen vereist dat de maatregelen die bij voorgaande niveaus horen, periodiek worden geëvalueerd en beoordeeld op effectiviteit. Er is sprake van een volledige PDCA-verbetercylcus (Plan-Do-Check-Act). Men is bewust bekwaam.

1.4.5 Het streven naar niveau 5

- Niveau 5 is het hoogste haalbare/meetbare niveau van het volwassenheidsmodel. Hierbij zijn bepaalde ondersteunende tools en processen van cruciaal belang, maar die komen pas in beeld als de basis (lagere niveaus) solide en herhaalbaar is. Men is onbewust bekwaam.
- Op niveau 5 wordt de bescherming van persoonsgegevens als een vanzelfsprekendheid gezien en wordt gekeken naar integraliteit met andere relevante disciplines zoals informatiebeveiliging, informatiemanagement en -beheer en integraal veiligheids- en risicomanagement.
- Bewijsvoering voor het bereiken van niveau 5 kan uitdagend zijn. Denk hierbij aan het documenteren van vergaderverslagen of rapportages.
- Sommige maatregelen of principes van een hoger niveau kunnen ook relevant zijn voor een lager niveau. Een voorbeeld hiervan is de proactieve houding van het bestuur, die een eis is voor niveau 5. Het is mogelijk dat een organisatie/bestuur die houding al heeft, zelfs als de organisatie nog volwassenheidsniveau 2 scoort.
- Stimuleren vanuit de top van de organisatie is altijd helpend, inclusief voorbeeldgedrag om het ambitieniveau te verwezenlijken.

1.5 Overwegingen volwassenheidsniveaus privacykader

De volgende overwegingen zijn van belang bij deze privacy-volwassenheidsniveaus:

- 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.

1.6 Rapportage benchmark SURFaudit

De resultaten uit de benchmark worden gebruikt voor analyse en rapportage. SURFaudit levert daarvoor drie verschillende rapportages:

Type rapport	Inhoud	Met wie wordt het gedeeld?
1 - Rapport per organisatie	Resultaten van de individuele organisatie en een vergelijking met organisaties binnen dezelfde sector, en met de totale populatie. Bijvoorbeeld: een hogeschool kan haar eigen score zien, vergeleken met alle andere hogescholen en met alle organisaties die deel hebben genomen aan de benchmark.	SURF deelt dit rapport **alleen** met de deelnemende organisatie.
2 - Sectorbeeld	Een uitgebreid rapport dat een overzicht geeft van de stand van zaken binnen de sector en per deelsector met een koepel van is. *Bijvoorbeeld: de koepel Universiteiten van Nederland, Vereniging Hogescholen, MBO Digitaal.* De resultaten van individuele organisaties zijn niet herleidbaar.	SURF deelt het rapport met koepelorganisaties en (deelnemende) organisaties die onder de koepel vallen.
3 – Benchmark rapport	Een kort openbaar rapport dat gemiddelden laat zien. Het algemene rapport bevat conclusies en aanbevelingen voor de gehele sector onderwijs en onderzoek en is geschikt voor algemene verspreiding.	Openbaar beschikbaar rapport.

2 Scope voor privacyaudit bepalen

2.1 Inleiding

In de context van een audit is de **scope** het gebied of de gebieden van de organisatie die worden beoordeeld op de 'privacy', de bescherming van persoonsgegevens (AVG). Het vaststellen van de scope is belangrijk omdat hiermee vooraf wordt vastgelegd hoe diep en hoe breed de audit wordt uitgevoerd. Dit is een belangrijk 'startpunt' om tot een goede/gedegen audit(-aanpak) te komen.

Er zijn verschillende manieren om de scope te bepalen. Op hoofdlijnen wordt naar organisatieaspecten en (verwerkings-)processen gekeken. In het geval van processen wordt bij informatiebeveiligingsaudits dan al snel naar IT-systemen ('kroonjuwelen') gekeken en de processen daaromheen. Bij privacyaudits kijken we naar de mate van bescherming van rechten en vrijheden van personen en draait alles om de verwerking(-sprocessen) van persoonsgegevens. In de basis gaat het hier om verwerkingen van persoonsgegevens binnen die processen. Behalve de organisatorische aspecten (beleid en inrichting) rondom privacy worden ook de aspecten rechten van betrokkenen, gegevensbescherming/incidenten en verantwoording getoetst.

2.2 Processen

De drie belangrijkste (hoofd-/) bedrijfsprocessen /-domeinen binnen de sector zijn **onderwijs, onderzoek en bedrijfsvoering** waarbij de processen binnen onderwijs, onderwijslogistiek/-ondersteuning en bedrijfsvoering voor alle organisaties op hoofdlijnen vergelijkbaar zijn. Binnen deze processen worden veel persoonsgegevens verwerkt. Denk daarbij aan die van (aspirant-) onderwijsdeelnemers (leerlingen, studenten en cursisten) en medewerkers (in dienst, inhuur, etc.).

Voor het hoger onderwijs biedt het bedrijfsprocesmodel van de HORA een overzicht van alle processen en voor het MBO is dit overzicht te vinden in het hoofdprocesmodel van de MORA.

2.2.1 Verwerking persoonsgegevens binnen onderwijsprocessen

Voorbeelden van (sub-)processen binnen het onderwijs en onderwijs-ondersteuning/-logistiek waarbinnen persoonsgegevens worden verwerkt (*In-, Door- & Uitstroom*) zijn:

- Studentenwerving.
- Het inschrijfproces (oriënteren, aanmelden, toelaten en in- & uitschrijven).
- Planning & roostering.
- Toetsen en beoordelen/studievoortgangsadministratie en examineren/diploma's
- Studentbegeleiding (zoals studentendecanen, studievertraging en -ondersteuning).
- Stage-& afstudeerbegeleiding.
- Beroeps Praktijk Vorming (mbo).
- Studentenportfolio.
- Alumni-administratie/-beheer.

2.2.2 Verwerking persoonsgegevens binnen onderzoek

Als bij (wetenschappelijk) onderzoek persoonsgegevens betrokken zijn, is de AVG van toepassing. Onderzoek komt in grote verscheidenheid voor. Het kan onder andere gaan om prospectief mensgebonden onderzoek, retrospectief onderzoek, hergebruik van gegevens of gebruik van publieke data, social media, longitudinaal onderzoek, kortlopende enquêtes en ook onderzoek met dieren. Voor onderzoek geldt daarnaast bijzondere regelgeving in het kader van mensgebonden onderzoek de verplichte betrokkenheid van een Medisch Ethische commissie (METC), de Nederlandse gedragscode wetenschappelijke integriteit (NWO 2016) en mogelijk de Wet geneeskundige behandelingsovereenkomst (WGBO) als er gezondheidsgegevens zijn betrokken. Onderzoek vindt plaats in diverse vormen en samenwerkingsverbanden, door (buiten) promovendi, hoogleraren en door PhD studenten.

De kaders van de AVG voor het gebruik van persoonsgegevens voor onderzoek leveren voor betrokken partijen nog interpretatievraagstukken. Zie de Handreiking Persoonsgegevens in Onderzoek voor handvatten op dit gebied.

2.2.3 Verwerking persoonsgegevens binnen de processen van bedrijfsvoering

Ook binnen bedrijfsvoering zijn er veel processen waarin persoonsgegevens worden verwerkt, waaronder:

- Personeelsadministratie (o.a. werving en selectie, beoordeling, ziekte- en verlofregistratie).
- Financiën (salarisadministratie, reiskosten, debiteuren waaronder studenten en leveranciers).
- Business intelligence/managementinformatie (verzamelen en analyseren van bedrijfsgegevens en bedrijfsinformatie uit bronsystemen/verschillende platformen/datasets).
- Facilitaire diensten ((Roostering,) zaalreservering, parkeren, elektronisch passen/sleutelsysteem, cameratoezicht, meten ruimtebezetting).
- Communicatie & marketing.
- Generieke ICT-diensten waaronder Identity management, logging & monitoring, etc.

2.3 Risico-gebaseerde scopebepaling

De AVG gaat uit van een risico-gebaseerde aanpak bij de verwerking van persoonsgegevens. Het is dus van belang om de processen en verwerkingen waar de risico's het grootst zijn als eerste inzichtelijk te maken. Om die reden wordt dan ook geadviseerd om een risico-gebaseerde aanpak te hanteren bij het bepalen van de auditscope.

2.3.1 Aanpak voor risico-gebaseerde scopebepaling

De eerdergenoemde procesmodellen van de HORA en MORA geven inzicht (mits gehanteerd) in de bedrijfsprocessen. De HORA- en MORA-applicatiemodellen geven daarbij meer detailinzicht in waar de persoonsgegevens worden verwerkt. Deze bieden samen een goede basis om de auditscope te bepalen.

Risico's identificeren– Bij de verwerking van persoonsgegevens onderzoekt een organisatie welke (privacy)risico's de verwerking met zich meebrengt. Tijdens de risicobeoordeling wordt duidelijk welke verwerkingen in welke processen plaatsvinden (inclusief in welke applicaties die verwerking plaatsvindt) en in welke mate deze verwerkingen risico's opleveren (zie de risicofactoren hieronder).

Deze risicobeoordeling hangt samen met PR.04 (een eerste risicoinschatting), PR.05 (privacybeoordeling) en PR.06 (Privacy by Design/Privacy Applicatie Assessment) van het privacykader. Bij de eerste risicoinschatting voer je een privacyclassificatie uit. Daarbij wordt onder andere gekeken naar grootte, gevoeligheid en complexiteit van een verwerking. Deze risicobeoordelingen helpen om de prioriteiten te stellen voor de scopebepaling.

Prioriteitsstelling: Op basis van de resultaten van de risicoafweging, bepaal je welke processen of verwerkingen je wilt laten toetsen via de audit. In de planning voor een volgend auditcyclus kun je processen en verwerkingen meenemen die buiten scope zijn gebleven.

Risicofactoren zijn:

Risicofactor	Toelichting
Volume van persoonsgegevens	De hoeveelheid persoonsgegevens die in een (deel-) proces worden verwerkt. Dit geldt voor zowel veel personen waarvan enkele persoonsgegevens verwerkt worden, als bij veel persoonsgegevens van enkele personen waarop de risico-afweging plaatsvindt.
Gevoeligheid van de gegevens	Niet alle gegevens zijn gelijk; bijzondere persoonsgegevens, bijvoorbeeld gegevens met betrekking tot gezondheid zijn gevoeliger dan basiscontactinformatie. Let hierbij ook op de context, dit kan met zich meebrengen dat persoonsgegevens gevoeliger zijn.
Is er sprake van geautomatiseerde individuele besluitvorming /gebruik van AI of algoritmes waaronder profilering	In beginsel is dit niet toegestaan. Als hier (toch) sprake van is en er geen inzicht is in de gebruikte algoritmen, vergroot dit de risico's.
Aantal mensen dat toegang heeft	Hoe meer mensen toegang hebben, hoe groter het risico op b.v. werkfouten/datalekken.
Risico van blootstelling	De kans dat de gegevens onbedoeld openbaar worden gemaakt of worden blootgesteld aan onbevoegden.
Complexiteit van de gegevensverwerkingsprocessen	Ingewikkelde processen met meerdere stappen of interacties tussen systemen brengen meer risico's met zich mee.

Risicofactor	Toelichting
Verwerking in derde landen	Worden de gegevens in derde landen verwerkt, met name in landen waarvoor geen adequaatheidsbesluit is genomen.
Gezamenlijke verantwoordelijkheid	Gezamenlijke verwerkingsverantwoordelijkheid kan risico verhogend werken, b.v. wanneer er geen goede onderlinge afspraken worden gemaakt.
Voorgeschiedenis incidenten	Hebben er in het verleden privacy- of beveiligingsincidenten plaatsgevonden. Deze zijn geregistreerd. Is ervan geleerd en/of is er actie ondernomen om herhaling te voorkomen?
Externe toegang	Hebben externe partijen toegang tot de gegevens? Bijvoorbeeld, cloudproviders, externe consultants, of partners.
Inzicht van procesverantwoordelijken/-eigenaren	Betrek procesverantwoordelijken/-eigenaren en vraag waar ze zich het meest zorgen over maken. Hun dagelijkse ervaring en kennis van operationele uitdagingen kan van onschatbare waarde zijn. Betrek ook systeemeigenaren/-verantwoordelijken en/of functioneel beheerders en/of procescoördinatoren.
(Ontbrekende) feedback van privacyfunctionarissen	Zij hebben een grondig begrip van privacy-uitdagingen en vraagstukken/casuïstiek binnen de organisatie. Hun input kan essentiële gebieden van aandacht en potentiële risico's blootleggen die anders over het hoofd kunnen worden gezien.

2.4 Overige aanbevelingen voor scopebepaling:

Afhankelijk van de structuur en omvang van de organisatie kan de scope verschillen. Processen zijn niet overal op dezelfde manier ingericht. Sommige organisaties zijn vrijwel geheel centraal georganiseerd en andere zijn sterker gedecentraliseerd of hebben de decentrale afdelingen met eigen processen waarin persoonsgegevens worden verwerkt.

3 Scope benchmark SURF Toetsingskader Privacy

Scope audit
Organisaties maken normaal gesproken een eigen risico-gebaseerde afweging om te bepalen welke processen (waarin persoonsgegevens worden verwerkt) men binnen de scope van de audit wil opnemen.

Scope benchmark
Voor de benchmark met de resultaten van het privacykader wijken we hier vanaf omdat de resultaten goed vergelijkbaar moeten zijn. Daarom is het belangrijk dat iedere organisatie die aan de benchmark meedoet dezelfde vergelijkbare processen toetst.

De scope voor de benchmark van het privacykader bestaat uit de volgende zeven generieke privacy-onderwerpen:

a. Beleid
b. Processen
c. Organisatorische inbedding
d. Rechten van betrokkenen
e. Samenwerking
f. Beveiliging
g. Verantwoording

We kijken hierbij naar de implementatie van het privacykader qua opzet, bestaan en werking. (VWN 3 is hierbij het uitgangspunt). Voor het complete overzicht van controls met bijbehorende statements, zie het toetsingskader via pec.surf.nl.

Als processen en procedures binnen deze processen (deels) zijn gedecentraliseerd, moeten de centrale organisatie en tenminste één decentrale eenheid worden getoetst.

3.1 Samenvatting scope

Hanteer de volgende scope bij een eerste deelname aan de benchmark:

- Proces (pre) DPIA
- Proces verwerkingsregister
- Proces datalekken
- Niveau van awareness en hoe het terugkerende karakter wordt geborgd
- Aanwezigheid van privacybeleid en gerelateerde afspraken en de naleving hiervan
- Proces privacygovernance en hoe dit is uitgerold en geborgd in de organisatie
- Proces rechten van betrokkenen
- Proces leveranciersmanagement en aanwezigheid van verwerkersovereenkomsten
- Proces rondom verwerkingen buiten de EER en de aanwezigheid van een ingericht proces, benodigde en documenten
- Proces rondom Privacy by Design/Default
- Proces rondom informatiebeveiliging (dit wordt opgepakt door het securityteam waar je mee samenwerkt)
- Proces rondom rapportagelijnen

Met deze meer generieke scope meet je een aantal aspecten van de AVG-vereisten, maar kijk je minder diep in de verwerkingen van persoonsgegevens binnen de (o.a. genoemde) primaire processen waardoor je bijvoorbeeld niet weet of je alle verwerkingen en alle risico's in beeld hebt.

4 Audittechnieken

De meest gebruikte audittechnieken zijn:

- onderzoek – via interviews met management en medewerkers), observatie (observatie van processen),
- observatie – observeren van processen/procedures
- inspectie – bekijken van beleid, procesbeschrijvingen, procedures, configuraties, etc.) en
- herhaling – ‘re-performance/heruitvoering, het opnieuw uitvoeren van een proces of procedure).

4.1 Onderzoek

Onderzoek is het proces van het rechtstreeks verzamelen van informatie van een manager of medewerker die bekend is met het onderwerp of de maatregel die wordt getest. Het onderzoek kan schriftelijk (bijvoorbeeld via e-mail) of mondeling (interviews) plaatsvinden. Deze methode wordt altijd toegepast in combinatie met observaties en inspecties en kan worden gebruikt om basiskennis van (complexe) processen te krijgen.

4.2 Observatie

Observatie is het proces van het observeren van processen of procedures die plaatsvinden. Een voorbeeld hiervan: verifiëren dat bepaalde processen en geautomatiseerde controles bestaan en werken zoals beschreven (dit kan overlappen met heruitvoering).

4.3 Inspectie

Inspectie is het onderzoeken van documentatie als bewijs dat er een maatregel aanwezig is/wordt uitgevoerd. Inspectie omvat vaak het verzamelen van beleid, procesbeschrijvingen, procedures en meldingen, verwerkingsregister en dergelijke. Een voorbeeld hiervan: verifiëren dat de verwerkingen binnen processen in scope volledig en actueel zijn opgenomen in het verwerkingsregister. Of inzage in de afhandeling van datalekken en registratie in het datalekregister.

4.4 Herhaling (heruitvoering)

Herhaling is het onafhankelijk recreëren van een proces om te controleren of het effectief werkt. Opnieuw uitvoeren kan ook het opnieuw creëren van een proces in combinatie met een observatie omvatten om een verder geautomatiseerd proces te observeren. Herhaling biedt over het algemeen de hoogste mate van zekerheid dat een proces aanwezig is en effectief werkt.

Om een vollediger en betrouwbaarder beeld te krijgen raden we de auditor aan om verschillende audittechnieken te gebruiken.

5 Auditmethodiek – stappenplan

5.1 Stap 1 – Voorbereiden

- Opdrachtgever

Het College van Bestuur van de instelling geeft opdracht tot het uitvoeren van een audit aan een interne functionaris vanuit de derde lijn (bijvoorbeeld Audit & Control) of een externe partij). De FG kan op eigen initiatief audits uit (laten) voeren. De Raad van Toezicht wordt geïnformeerd over de uitkomsten.

N.B. Interne audit - afdelingen en proces- of lijnmanagers kunnen binnen hun mandaat ook opdracht geven tot het uitvoeren van een audit. Deze audits hebben meestal een beperkte scope.

- Auditdoelstelling

Bij het geven/verlenen van de opdracht wordt de auditdoelstelling geformuleerd:
“Stel vast wat het volwassenheidsniveau van de instelling is op het gebied van privacy, wat de grootste risico’s zijn, en welke verbeteringen aangebracht moeten worden om de risico's te reduceren en de volwassenheid te verhogen”. Gebruik hiervoor het SURFaudit toetsingskader privacy en hanteer de scope en diepgang zoals beschreven in deze aanpak.

- Auditcoördinator

Voor het uitvoeren van een externe audit is een coördinator/projectmanager nodig die op onafhankelijke wijze de audit begeleid, interviews plant en de doorlooptijd monitort. Bij voorkeur is dit niet de persoon of organisatie die wordt geaudit, maar bijvoorbeeld iemand uit de afdeling Internal Audit of een projectleider met een audit-achtergrond.

5.2 Stap 2 – Type audit

Bij de opdrachtformulering wordt ook het type audit vastgesteld, een self-assessment (al dan niet met peer review), een interne audit of externe audit. Daarnaast kan het type audit verder worden ingekaderd door in de opdrachtomschrijving al aan te geven welke audittechnieken gebruikt gaan worden (onderzoek, observatie, inspectie, herhaling).

5.3 Stap 3 – Uitvoeren

- De auditor stelt, in samenspraak met de auditcoördinator, een auditplan op,
- De auditcoördinator bewaakt de voortgang van de audit en intervenieert als nodig. Hij/zij rapporteert over de voortgang aan zijn/haar opdrachtgever op basis van de gespreksverslagen. Alle bevindingen worden middels hoor-wederhoor met de geïnterviewden, de audit coördinator en het verantwoordelijk management afgestemd alvorens gerapporteerd wordt.

Scoringsmethodiek

- Het volwassenheidsniveau wordt alleen toegekend als aan alle eisen bij betreffende statement/beheersmaatregel voor dat volwassenheidsniveau aantoonbaar is voldaan. Als

dat niet het geval is wordt de score van het voorliggende volwassenheidsniveau toegekend. Er worden derhalve geen halve punten per beheersmaatregel / control toegekend.
- N.B. Het gemiddelde eindcijfer per domein en het overall gemiddelde eindcijfer wordt afgerond op één tiende punt.
- N.B. Het gemiddelde eindcijfer wordt berekend door het optellen van alle resultaten van de individuele statements, gedeeld door het aantal statements die van toepassing zijn. (Dus niet door het optellen van de domein scores gedeeld door het aantal domeinen)

5.4 Stap 4 – Rapporteren

- In de rapportage worden alle bevindingen benoemd en worden kritieke tekortkomingen uitgelicht, zodat de instelling een verbeterplan kan maken om bevindingen met de grootste risico's als eerste aan te pakken. In de rapportage vermeldt de auditor zijn/haar conclusies en aanbevelingen. E.e.a. in relatie tot de opdracht.
- De (interne) auditrapportage bevat bij voorkeur de volgende elementen:
  - Een managementsamenvatting
  - De opdracht en scope van de audit (het onderwerp).
  - Hoe de audit is uitgevoerd.
  - Hoe de resultaten tot stand zijn gekomen.
  - Met wie is gesproken.
  - Welke documenten, formulieren en informatiesystemen zijn geraadpleegd.
  - Eventuele beperkingen (bijvoorbeeld vanwege het niet tijdig toegang krijgen tot vereiste informatie).
  - De resultaten met daarbij eventueel opvallende zaken, afwijkingen of tekortkomingen die zijn geconstateerd.
  - Eventuele aanbevelingen of afspraken over verbeterplannen (afhankelijk van de auditopdracht).

  Begin de managementsamenvatting met een conclusie en vermeld aandachtspunten. Vergeet niet om, waar mogelijk, positieve ontwikkelingen te noemen en complimenten te geven.
- Het rapport wordt door de auditor voorgelegd aan de opdrachtgever, nadat hoor en wederhoor heeft plaatsgevonden wordt deze definitief gemaakt/vastgesteld.
- Het SURF Toetsingskader Privacy dient als template voor het aanleveren van de instellingsresultaten voor de benchmark.
- SURF verzamelt de scores van alle instellingen, maakt een rapport en brengt gemeenschappelijke tekortkomingen in kaart, zodat die, waar mogelijk, gezamenlijk kunnen worden opgepakt. Resultaten zijn niet herleidbaar naar instellingen. Deze krijgen zelf wel een 1-op-1 terugkoppeling met vergelijk naar algehele resultaat per (deel-)sector.

5.5 Stap 5 – Borging

Op basis van de uitkomst van de audit stelt iedere instelling een verbeterplan vast. SURFaudit formuleert samen met de CPO's/PO's/SCIPR doelen/acties die gezamenlijk kunnen worden aangepakt.Het verbeterplan van de instelling wordt voorgelegd aan het CvB. Het Toetsingskader zelf wordt beheerd door SURF (Privacy Expertise Centrum) en wordt periodiek gereviewd (inclusief voorbeelden van het bewijsmateriaal als handreiking). In Bijlage 2 - zijn aandachtspunten voor nazorg opgenomen.

Bijlage 1 - Voorbeeldplanning (bij deelname aan benchmark)

SURFaudit organiseert jaarlijks de benchmark. De deadline voor het aanleveren van de resultaten is telkens op 31 januari (met de resultaten over het voorgaande jaar). Hoe beter de verbetercyclus werkt, hoe gemakkelijker de doorloop naar de definitieve rapportage/oplevering resultaat werkt.

Voorbeeldplanning

Onderdeel	Doorlooptijd	Actie
Audit uitvoeren	September	Scope bepalen
Rapporteren	1e week oktober	Kick-off (opdracht & scope) Uitvraag documentatie en plannen interviews
	2e en 3e week oktober	Documentatieonderzoek
	Laatste week oktober	Interviews/onderzoek
	1e en 2e week november	Verwerken resultaten (centraal/decentraal)
Rapporteren	2e en 3e week november	Conceptrapportage opstellen
	1e week decenmber	Conceptrapportage bespreken
	2e en 3e week december	Definitieve rapportage opstellen met advies FG
	Eind december/begin januari	Presentatie eindrapportage Akkoord portefeuillehouder
	Laatste twee weken van januari	Aanleveren resultaten (cijfers) aan SURF
Borging/PDCA	Januari/maart	Opstellen verbeterplannen Bestuurlijke borging
	Januari t/m december	Verbetercyclus opvolgen

Tip: probeer bij de planning van de audit rekening te houden met andere audits en stem dit van tevoren af.

Bijlage 2 - Aandachtspunten bij nazorg

Onderstaande lijst bevat algemene aandachtspunten voor het verbeteren van de bescherming van persoonsgegevens, los van eventuele verbeterpunten die uit de audit naar voren zijn gekomen. Deze punten helpen om de bescherming van persoonsgegevens te verbeteren als onderdeel van de verbetercyclus.

1. **Implementatie van het 'bescherming van persoonsgegevens'-programma** – Privacy (het beschermen van rechten en vrijheden van personen) is onderdeel van de normale bedrijfsactiviteiten en moet zijn ingebed in de cultuur van de organisatie. Het invoeren en monitoren van privacymaatregelen worden als vanzelfsprekend beschouwd, zodat de instelling een veilige studie- en werkplek is en blijft. Neem dit op in de PDCA-verbetercyclus.
2. **Beleidsdocumenten en richtlijnen** – Om te blijven voldoen aan relevante wet-&regelgeving, standaarden en interne regels worden beleidsdocumenten en richtlijnen up-to-date gehouden.
3. **Prestatie-indicatoren** – 'Meten is weten', prestatie-indicatoren helpen om middelen in te zetten daar waar ze het meest nodig zijn. Zie het ook als manier het gesprek te voeren.
4. **Verantwoordelijkheid voor de bescherming van persoonsgegevens binnen processen en systemen** – Het management (proces- en lijnmanagers) is hier verantwoordelijk voor. Beleg dit duidelijk en vraag hen eigenaarschap te tonen. 'Tone at the top' en voorbeeldgedrag.
5. **Privacy en Risk Management** – Blijven voldoen aan relevante wet-&regelgeving, standaarden en interne regels is geen doel op zich. De focus dient te liggen op een organisatiecultuur waarbij het beschermen van persoonsgegevens vanzelfsprekend is. Het voldoen aan standaarden en interne regels is daarvan een gevolg.
6. **Continu monitoren van het effect van privacymaatregelen** – Monitor en test maatregelen en activiteiten continu op effectiviteit, efficiëntie en gevolgen en documenteer de bevindingen.
7. **Detecteer en reageer op niet-effectieve privacymaatregelen** – Er is een proces om niet-effectieve maatregelen te signaleren en bij te stellen. Wanneer een maatregel niet effectief blijkt, wordt hierop direct actie ondernomen. Hierdoor blijven de gevolgen minimaal. Er wordt een analyse gedaan naar de oorzaak en de maatregel wordt aangepast of aangevuld met additionele maatregelen. Sla b.v. de evaluatie van een datalek niet over.
8. **Privacybewustwording** – Social engineering en andere middelen van actoren (b.v. phishing) leiden vaak tot datalekken en exfiltratie van gevoelige data. Het (periodieke) awareness programma wordt steeds up-to-date gehouden aan de hand van recente security- & privacy-incidenten en trends. Start bij nieuwkomers/introductie (onboarding).
9. **Bescherming van persoonsgegevens door externe dienstverleners** – Wanneer een instelling gebruik maakt van externe dienstverleners (generaliserend kan dat van cloudleverancier tot bloemist zijn) is er een proces om te monitoren of deze externe dienstverleners adequate maatregelen hebben getroffen voor de bescherming van persoonsgegevens en, als nodig, contractuele afspraken hierover bij te stellen. Gezamenlijke audit van/bij een leverancier?
10. **Evolutie van het privacyprogramma** – Maatregelen worden aangepast naar aanleiding van veranderingen en trends in het dreigingslandschap, veranderingen bij de instelling zelf en nieuwe ontwikkelingen in de wet- en regelgeving, zodat die geen negatieve gevolgen hebben voor de instelling. Hanteer hiervoor bijvoorbeeld sectorale dreigingsbeelden en informatie van de AP.

Bijlage 3 - Definities

Term	Definitie
Audit	Een audit is een systematisch, onafhankelijk en gedocumenteerd proces/onderzoek om relevant en passend bewijsmateriaal te verzamelen en dat op objectieve wijze te beoordelen om vast te stellen in welke mate is voldaan aan de auditcriteria[1].
Opzet	Processen zijn beschreven (ontwerp/concept).
Bestaan	Processen functioneren (eenmalig getoetst/vastgesteld).
Werking	Processen werken altijd zoals bedoeld en zijn effectief voor een bepaalde periode. De verbetercyclus is ingesteld of er heeft een evaluatie plaatsgevonden.
Opdrachtgever	Het is belangrijk om vast te stellen wie *opdrachtgever* is voor het uitvoeren van de audit. Met de opdrachtgever wordt besproken wat de *scope* van de audit is en de opdrachtgever krijgt ook de resultaten van de audit. Het ligt voor de hand dat het bestuur van de organisatie opdrachtgever is, maar ook de FG of een lijn- of proces-manager (of interne auditor of controller) kunnen binnen hun mandaat opdrachtgever zijn.

Er zijn meerdere manieren om een audit of onderzoek uit te voeren naar opzet, bestaan en werking van beheersmaatregelen. Hieronder (schema) staan ze opgenomen waarbij van boven naar beneden de objectiviteit van het onderzoek hoger wordt:

Term	Definitie
Self-assessment	Een onderzoek uitgevoerd door (lijn- of proces-) verantwoordelijke afdelingen/entiteiten, daarbij waar nodig geholpen door privacy officer(s) en andere tweedelijns deskundigen, met als doel te meten in hoeverre de verbeterdoelen worden gehaald of om te meten wat de huidige status is.
Interne audit	Een audit uitgevoerd vanuit een derdelijns-positie zoals de interne auditafdeling is onafhankelijk en biedt het bestuur met behulp van eigen onderzoeken zekerheid over de mate waarin doelstellingen en beheersmaatregelen gerealiseerd worden en/of huidige status (b.v. op basis van een toetsingskader). De interne auditor is doorgaans bekend met de processen binnen de organisatie.
Externe audit	Een audit uitgevoerd door een externe (onafhankelijke) auditor die weinig of geen kennis van en geen arbeidsrelatie of -overeenkomst met de organisatie heeft. Dit type audit geeft het bestuur zicht op de aantoonbaarheid van beheersmaatregelen.

[1] https://www.nen.nl/managementsystemen/auditing-iso-19011 Richtlijn voor intern auditen