Samen aanjagen van vernieuwing

Handreiking auditverplichting verwerkers

Risicogestuurde controle bij leveranciers volgens artikel 28 AVG

Colofon

Het doel van dit document is een handreiking te bieden voor de praktische, risicogestuurde omgang met de auditverplichting volgens artikel 28 van de AVG bij verwerkers (leveranciers).

Bestemd voor

Dit document is bestemd voor privacyprofessionals, managers en andere bij de risicobereidheid en -beheer betrokken medewerkers.

Samenstelling en beheer

Dit document is gebaseerd op de voormalige bijlage D bij het SURF Juridisch Normenkader (JNK) uit 2018 en is tot stand gekomen via het Privacy Expertise Centrum van SURF. Het beheer van deze handreiking berust bij SURF.

Licentie

Versiebeheer **Privacykader SW.01**

Versie	Door	Datum	Toelichting/wijziging
1.0	SURF PEC	Februari 2026	Initieel document

Inhoudsopgave

1. Inleiding **4**

Doelstelling **4**

2. De auditverplichting **4**

Elementen auditverplichting **5**
Auditfrequentie **5**

3. Bepalen of je kunt afwijken van de auditverplichting **6**

Stap 1 – Privacyclassificatie (GGC-classificatie) **6**
Stap 2 – Knock-outs vaststellen **7**

4. Manieren van afwijken van de auditverplichting **8**

1. Inleiding

Volgens de AVG moet een verwerkingsverantwoordelijke op ieder willekeurig moment kunnen aantonen dat de wet wordt nageleefd. Dat geldt ook als een verwerking van persoonsgegevens is uitbesteed aan een derde partij, de zogenaamde 'verwerker'. Met de verwerker worden afspraken gemaakt over de bescherming van deze verwerking (meestal via een verwerkersovereenkomst).

De bij SURF aangesloten instellingen maken gebruik van verschillende leveranciers. Leveranciers verschillen sterk in grootte, aard en bestaanshistorie van de organisatie. Ook verschilt de aard van geleverde diensten en de gevoeligheid van de verwerkte gegevens. Een one-size-fits-all-oplossing is daarom niet haalbaar. De diversiteit maakt het noodzakelijk om te kunnen variëren in de aanpak van de auditverplichting. Deze handreiking geeft daar handvatten voor.

Doelstelling

Het doel van dit document is een handreiking te bieden voor de praktische, risicogestuurde omgang met de auditverplichting volgens artikel 28[1] van de AVG bij verwerkers (leveranciers).

2. De auditverplichting

Onderwijsinstellingen gebruiken het Toetsingskader Privacy[2] en het Toetsingskader Informatiebeveiliging[3] als met volwassenheidsniveau 3 als norm voor gegevensbescherming van verwerkingen van persoonsgegevens. Een organisatie moet als (verwerkings)verantwoordelijke aantoonbaar in control moet zijn bij die gegevensbescherming. Dat geldt ook als een verwerker (leverancier) de verwerking namens de organisatie verzorgt.

Met leveranciers worden afspraken gemaakt over de eisen voor informatiebeveiliging en privacy via de verwerkersovereenkomst (doorgaans als bijlage bij de hoofdovereenkomst voor de dienstverlening). In deze verwerkersovereenkomst is de wettelijke vereiste onafhankelijke auditverplichting opgenomen. Het doel is dat de opdrachtgever c.q. de verwerkingsverantwoordelijke kan controleren of de leverancier (en eventuele subverwerkers) voldoet aan alle afspraken en verplichtingen van de AVG andere toepasselijke wet- en regelgeving op het gebied van privacy in de hoofd- en de verwerkersovereenkomst.

Van de leverancier wordt gevraagd om periodiek een onafhankelijke IT-auditor of deskundige onderzoek te laten doen naar de bescherming van de persoonsgegevens. Naast de periodieke audit die de verwerker zelfstandig laat uitvoeren, kan de verwerkingsverantwoordelijke een audit laten uitvoeren bij de verwerker.

[1] Zie Artikel 18, lid h & overweging 81, Inzet van verwerkers
[2] Toetsingskader Privacy (pec.surf.nl)
[3] Toetsingskader Informatiebeveiliging (sec.surf.nl)

Elementen auditverplichting

In het SURF-model Verwerkersovereenkomst 4.0 is voor de auditverplichting het volgende opgenomen (letterlijk, inclusief onjuiste doorlopende nummering):

ARTIKEL 8 AUDIT

8.1 Verwerker stelt aan Verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om de naleving van de verplichtingen uit deze Verwerkersovereenkomst aan te tonen. Verwerker stelt jaarlijks een auditrapport op waarin hij aantoont dat hij voldoet aan de verplichtingen uit deze Verwerkersovereenkomst en verstrekt deze op verzoek. Dit rapport wordt opgesteld door een onafhankelijke, deskundige derde partij en is voorzien van een verklaring dat de bevindingen een getrouw beeld geven van de werkelijkheid. Indien concrete omstandigheden naar het oordeel van Verwerkingsverantwoordelijke daartoe aanleiding geven of indien Verwerkingsverantwoordelijke vermoedt dat Verwerker zijn verplichtingen niet nakomt, kan Verwerkingsverantwoordelijke alsnog een eigen audit (laten) uitvoeren. Verwerker zal daar zijn medewerking aan verlenen, onder meer door het verlenen van toegang tot systemen en documenten. De kosten van een eigen audit zijn voor rekening van Verwerkingsverantwoordelijke, tenzij uit de audit blijkt dat Verwerker tekort is geschoten in de nakoming van zijn verplichtingen uit deze Verwerkersovereenkomst.

8.3 – Verwerkingsverantwoordelijke meldt de audit minstens veertien (14) dagen van tevoren. De audit zal de normale bedrijfsactiviteiten van Verwerker niet onredelijk verstoren.

8.4 - Verwerkingsverantwoordelijke behandelt de uit de audit verkregen informatie vertrouwelijk en deelt deze alleen met die samenwerkingspartners voor wie kennisname van de informatie redelijkerwijs noodzakelijk is. Verwerkingsverantwoordelijke noch de hiervoor bedoelde samenwerkingspartners zullen de auditresultaten openbaar maken of met derden delen, tenzij dit wettelijk vereist is.

8.5 - Als uit de audit blijkt dat Verwerker niet aan zijn verplichtingen uit deze Verwerkersovereenkomst voldoet, neemt Verwerker direct en op eigen kosten alle redelijke maatregelen om te zorgen dat Verwerker alsnog aan deze verplichtingen voldoet.

Deze auditverplichting betekent:

1. **Periodiek onderzoek** - De verwerker is verplicht periodiek een onafhankelijk onderzoek te laten uitvoeren om aan te tonen dat de afspraken op het gebied van gegevensbescherming worden nageleefd.
2. **Auditrapport** - De verwerker zorgt ervoor dat de onafhankelijke partij van de bevindingen een rapport opstelt en stelt dit op verzoek aan de verwerkingsverantwoordelijke.
3. **Eigen onderzoek** – De verwerkingsverantwoordelijke kan een eigen onderzoek uitvoeren als dat nodig wordt geacht. In zo'n geval meldt de organisatie dit ten minste veertien dagen van tevoren bij de leverancier.
4. **Geheimhouding** – De auditresultaten worden vertrouwelijk behandeld door de betrokken partijen.
5. **Maatregelen om te voldoen** – Als de auditresultaten aangeven dat er onvoldoende maatregelen zijn getroffen, zorgt de verwerker er op eigen kosten voor dat de extra benodigde maatregelen zo snel mogelijk worden geïmplementeerd.

Auditfrequentie

De frequentie van deze audit hangt af van het risico van de verwerking:

Hoog risico : jaarlijks (bijvoorbeeld bij de verwerking van bijzondere persoonsgegevens)
Middel risico : tweejaarlijks
Laag risico : geen verplichting tot audit/periodiek onderzoek

Om de frequentie te kunnen bepalen, moet een risico-inschatting worden uitgevoerd. Om dat op de juiste manier te doen, kijk je o.a. naar de gevoeligheid van de gegevens (het vertrouwelijkheidslabel)[4] en de mogelijke impact[5] op de belangen, rechten en vrijheden van de betrokken personen als er iets misgaat met de persoonsgegevens (datalek). Blijkt uit de inschatting dat het risico laag is, dan vervalt de auditverplichting. Leg de verantwoording voor de risicoclassificatie vast, zodat later terug te redeneren is waarom voor een bepaalde auditfrequentie is gekozen.

3. Bepalen of je kunt afwijken van de auditverplichting

Soms voldoet een leverancier (nog) niet aan de auditverplichting. Dit hoofdstuk beschrijft wanneer, onder welke voorwaarden en hoe je tijdelijk kunt afwijken van de standaard-auditverplichting.

Stap 1 – Privacyclassificatie (GGC-classificatie)

Een basisinschatting van het privacyrisico kun je maken met behulp van de privacyclassificatie. Qua opzet en bruikbaarheid is de classificatie vergelijkbaar met de BIV-classificatie die wordt gebruikt voor informatiebeveiliging:

- de BIV-classificatie helpt om het benodigde beschermingsniveau vast te stellen aan de hand van de onderdelen Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van informatie
- de GGC-classificatie om het privacyrisico van de verwerking beter in te schatten. Je kijkt naar een paar andere onderdelen, namelijk: Grootte, Gevoeligheid en Complexiteit (GGC) van de verwerking. Voor deze GGC-classificatie, zie de SURF PEC-website[6].

Met de GGC-classificatie kun je beter beoordelen welke mogelijkheden je hebt om te variëren/afwijken op basis van de knock-outs (zie stap 2).

Tabel overzicht onderdelen GGC-classificatie

Criterium	Risico L/M/H
G - Grootte	
Aantal betrokkenen	
Volume van de soorten persoonsgegevens	
Aantal mensen met toegang intern	
Aantal mensen met toegang extern	
Technische beveiligingsmaatregelen	
G - Gevoeligheid	
Vertrouwelijkheidslabel	
Impact op rechten of vrijheden betrokkene	
Privacyrisico door blootstelling	
C - Complexiteit	
Complexiteit van het proces	
Aantal subverwerkers	
Gebruik van AI	
Privacy by Design	

[4] Vertrouwelijkheidslabel (pec.surf.nl)
[5] Risico-inschatting van de verwerking (pec.surf.nl)
[6] Privacyclassificatie (pec.surf.nl)

Stap 2 – Knock-outs vaststellen

Aan de hand van een set criteria, de zogenaamde knock-outs, kun je beoordelen of je kunt variëren/afwijken van de auditverplichting. Blijkt uit de GGC-classificatie dat een knock-out voorkomt in de score, dan betekent het dat afwijken/variatie niet wenselijk is.

De organisatie bepaalt zelf de eigen criteria en kijkt of combinaties van bepaalde criteria tot een knock-out leiden (bijvoorbeeld als er 3x Midden wordt gescoord kan dat ook als knock-out gelden).

Hieronder vind je de tabel met knock-outs op basis van de privacyclassificatie (GGC). In deze is een voorzet als suggestie gegeven van de criteria die in ieder geval tot een knock-out moeten leiden.

Criterium	**Knock-out**
G - Grootte	
Aantal betrokkenen	
Volume van de soorten persoonsgegevens	
Aantal mensen met toegang intern	
Aantal mensen met toegang extern	
Technische beveiligingsmaatregelen	
G - Gevoeligheid	
Vertrouwelijkheidslabel	Hoog
Impact op rechten of vrijheden betrokkene	Hoog
Privacyrisico door blootstelling	
C - Complexiteit	
Complexiteit van het proces	Hoog
Aantal subverwerkers	
Gebruik van AI	Hoog
Privacy by Design	

Zodra één knock-out van toepassing is, is afwijken van de auditverplichting niet wenselijk. Is er geen knock-out van toepassing, dan weeg je de criteria in onderlinge samenhang. Probeer daarbij altijd risico's naar concrete voorbeelden te vertalen: wat kan er mis gaan?

Bijvoorbeeld:

- een score van Midden op het vertrouwelijkheidslabel en Midden op het volume van de soorten persoonsgegevens, of
- een combinatie van een groot aantal betrokkenen en een hoog volume van soorten persoonsgegevens kan tot een knock-out leiden.

Deze afweging helpt met de keuze op welke manier je eventueel verantwoord kunt afwijken. Je kijkt bij de afweging logischerwijs naar de context van de beoogde verwerking.

Je kunt altijd aanvullende criteria nemen, zoals het trackrecord van de leverancier, de locatie (jurisdictie) van de verwerking (als dit buiten de EER valt), innovatief karakter van de dienst, etc.

4. Manieren van afwijken van de auditverplichting

Allereerst is het van belang dat je de (tijdelijke) afwijking op de auditverplichting goed onderbouwt. Tref waar mogelijk maatregelen die de risico's zoveel mogelijk compenseren. Bewaar de onderbouwing en de compenserende maatregelen als bewijsmateriaal.

Je kunt uit een van de vier volgende varianten kiezen:

1. Een **tijdelijk uitgestelde audit** met compenserende maatregelen ter overbrugging. Kies een uitstel van zes tot maximaal twaalf maanden. Neem dit op in de afspraken (hoofdovereenkomst of verwerkersovereenkomst). Een compenserende maatregel is bijvoorbeeld een beschrijving van de opzet van de beveiligingsmaatregel die door de instelling wordt geaccordeerd.

2. Een **andere auditor** voert de audit uit (in plaats van de onafhankelijke ICT-auditor die werkt in opdracht van de leverancier), denk aan:

    a. Een externe ICT-auditor of deskundige die de instelling aanwijst en opdracht geeft.
    b. Eén of meerdere instellingen in opdracht van de leverancier.
    c. Een peeraudit (één of meerdere instellingen in opdracht van één of meerdere instellingen).
    d. Self-assessment op basis van de Toetsingskaders voor Informatiebeveiliging en Privacy van SURF.

3. Een **ander normenkader** voor de audit:
    a. Specifieke normenkaders (zoals ISO 27001).
    b. Specifiek benoemde Best Practice-bepalingen.

4. Een **andere focus**: niet het verrichten van een audit naar de werking van de maatregelen, maar uitsluitend onderzoek naar opzet en implementatie.