Handreiking Auditverplichting

SURF Juridisch Normenkader (Cloud)services, Bijlage D

Versie 2.0

Utrecht, maart 2018
Versienummer: 2.0

Colofon

Handreiking Auditverplichting
SURF Juridisch Normenkader (Cloud)services, Bijlage D

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

Inhoudsopgave

1. Inleiding

1.1. Achtergrond

In 2013 heeft SURF het SURF Juridisch Normenkader (Cloud)services (hierna: Normenkader) gepubliceerd, die is geüpdatet in 2016. In de kern bestaat het Normenkader uit best practice contractclausules op het gebied van vertrouwelijkheid, eigendom van data, beschikbaarheid en privacy.

Het zwaartepunt ligt daarbij op privacy. Het Normenkader is erop gericht dat de instelling de verwerkingsverantwoordelijke is voor de verwerking van persoonsgegevens, ook bij gebruik van een verwerker (leverancier). Dit betekent dat de instelling aantoonbaar in control moet zijn en blijven door middel van adequate overeenkomsten en adequaat nalevingstoezicht.

De Nederlandse meldplicht datalekken (in werking sinds 1 januari 2016)[1], de inwerkingtreding van het EU-VS Privacyshield per 12 juli 2016[2], de per 25 mei 2018 van kracht wordende Algemene Verordening Gegevensbescherming (AVG)[3] en de Nederlandse Uitvoeringswet Algemene verordening gegevensbescherming die tevens per 25 mei 2018 in zal gaan,[4] hebben geleid tot het actualiseren van privacy clausules. Om van het Normenkader een meer praktisch instrument te maken is er voor gekozen de geactualiseerde privacy bepalingen onder te brengen in een zogenaamde verwerkersovereenkomst. Deze Model Verwerkersovereenkomst is na vaststelling door de Juridische Commissie begin januari 2016 gepubliceerd. Een geactualiseerde versie van de verwerkersovereenkomst is in november 2017 ter beschikking gesteld op https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2017/model-verwerkersovereenkomst-surf-oktober-2017.pdf. Ook een Engelstalige versie is beschikbaar.[5]

Een belangrijke bepaling uit de verwerkersovereenkomst heeft betrekking op de beveiliging en stelt aan verwerkers de eis om een audit te laten uitvoeren. Van de verwerker wordt gevraagd om periodiek en op verzoek een door haar aan te wijzen onafhankelijke IT auditor of deskundige een onderzoek te laten uitvoeren ten aanzien van de organisatie van de verwerker, teneinde te doen vaststellen of de leverancier voldoet aan alle in de verwerkersovereenkomst en hoofdovereenkomst opgenomen verplichtingen met betrekking tot de AVG en andere toepasselijke wet- en regelgeving op het gebied van privacy. De frequentie van het onderzoek is een keer per twee jaar met uitzondering van verwerkingen met een hoog risico of een laag risico. Bij verwerkingen mag een hoog risico wordt jaarlijks een audit van verwerker gevraagd. Er is sprake van een hoog risico indien bijzondere persoonsgegevens in de zin van de AVG worden verwerkt. Indien er sprake is van een laag risico, geldt er geen verplichting tot het doen van een periodiek onderzoek. Naast de periodieke audit die de verwerker zelfstandig laat uitvoeren, kan de verwerkingsverantwoordelijke ook op zijn verzoek een audit laten uitvoeren bij de verwerker.

De bij SURF aangesloten instellingen maken gebruik van veel en zeer diverse leveranciers. Ook de diversiteit is zeer groot. Leveranciers verschillen bijvoorbeeld sterk naar grootte, aard en bestaanshistorie van de organisatie. Daarnaast zitten er verschillen in de aard van de door de leveranciers aan aangesloten instellingen geleverde diensten en de gevoeligheid van de daarmee verwerkte gegevens.

[1] Zie: http://wetten.overheid.nl/BWBR0037346/2015-12-16.
[2] Op het moment van publiceren van deze Handreiking, wordt het EU-VS Privacyshield nog beschouwd als zijnde een 'adequaat beschermingsniveau' in de zin van artikel 45 AVG. Wegens een lopende procedure bij het Hof van Justitie van de Europese Unie tegen het Privacy Shield, is het echter niet zeker of deze overeenkomst in stand zal blijven.
[3] Zie: http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32016R0679.
[4] Op het moment van publiceren van deze Handreiking, is het Wetsvoorstel voor de Uitvoeringswet Algemene verordening gegevensbescherming nog niet definitief. De verwachting is echter dat deze wet per 25 mei 2018 in Nederland van toepassing zal zijn.
[5] Zie: https://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2017/model-processor-agreement-english-surf-oktober-2017.pdf.

Deze diversiteit heeft tot gevolg dat het soms noodzakelijk is om te variëren in de toepassing van de auditverplichting. Een “one-size-fits-all” oplossing is – zeker in eerste instantie – niet altijd haalbaar.

1.2. Doelstelling

Het doel van dit document is om een handreiking te bieden voor de omgang met de auditverplichting in de praktijk op het moment dat verwerkersovereenkomsten worden gesloten tussen instellingen en leveranciers.

1.3. Leeswijzer

In hoofdstuk 2 wordt de auditverplichting in meer detail beschreven. Hoofdstuk 3 beschrijft vervolgens de leidraad voor het variëren op deze eis en geeft een opsomming van de relevante overwegingen en uitsluitingen hierbij. Indien dit leidt tot een andere invulling van de auditverplichting wordt afsluitend een aantal opties beschreven die in dat geval gehanteerd kunnen worden.

In de bijlage wordt de relevante wet- en regelgeving op hoofdlijnen beschreven.

2. Auditverplichting

Het Normenkader is erop gericht dat de instelling de (verwerkings)verantwoordelijke is voor de procesbeheersing, ook bij gebruik van een verwerker (leverancier). Dat betekent dat de instelling aantoonbaar in control moet zijn en blijven door middel van adequate overeenkomsten en adequaat nalevingstoezicht.

Ten aanzien van de beveiliging geeft het Normenkader regels voor:
- Passende maatregelen voor logische en fysieke beveiliging.
- Meld- en informatieplicht beveiligingsincidenten (bijv. verlies data).
- Reactieplicht: veiligstellen, voorkomen verdere onbevoegde handelingen.
- Medewerkingsplicht: informeren autoriteiten en betrokkenen.
- Informatieplicht (desgevraagd) over organisatie van verwerking en beveiliging persoonsgegevens.

De eis voor nalevingstoezicht is in het Normenkader vertaald in een onafhankelijke auditverplichting. Dit onafhankelijk onderzoek heeft ten doel om vast te stellen of de leverancier voldoet aan alle in de verwerkersovereenkomst en hoofdovereenkomst opgenomen verplichtingen met betrekking tot de AVG en andere toepasselijke wet- en regelgeving op het gebied van privacy. Belangrijke aspecten met betrekking tot de beveiliging van persoonsgegevens zijn de vertrouwelijkheid en integriteit (de weerstand tegen ongewenste aanpassingen of wissingen van persoonsgegevens) en de beschikbaarheid en veerkracht (het om kunnen gaan met storingen) van de door de leverancier ter beschikking gestelde diensten en systemen.

In de Model Verwerkersovereenkomst is de volgende bepaling opgenomen:

ARTIKEL 7. AUDIT

7.1 Verwerker is verplicht periodiek een onafhankelijke, externe deskundige een audit te laten uitvoeren ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Overeenkomst, de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet.

7.2 Verwerker verricht tenminste een keer per twee jaar een periodieke audit, zoals bedoeld in artikel 7.1 Indien Bijzondere categorieën Persoonsgegevens worden verwerkt, verricht Verwerker tenminste eenmaal per jaar een periodieke audit zoals bedoeld in artikel 7.1.

7.3 Verwerker is enkel niet gehouden tot het verrichten van een periodieke audit zoals bedoeld in artikel 7.1, indien Verwerker uitsluitend Persoonsgegevens verwerkt met een laag risico en uitdrukkelijk in Bijlage A is opgenomen dat Verwerker niet gehouden is tot het verrichten van een periodieke audit. Verwerkingsverantwoordelijke stelt vast of er sprake is van een laag risico.

7.4 Verwerker is verplicht de bevindingen van de onafhankelijke, externe deskundige, op verzoek aan Verwerkingsverantwoordelijke ter beschikking te stellen in de vorm van een verklaring, waarin de deskundige een oordeel geeft over de kwaliteit van de door Verwerker getroffen technische en organisatorische beveiligingsmaatregelen met betrekking tot de Verwerkingen die Verwerker ten behoeve van Verwerkingsverantwoordelijke verricht.

7.5 Verwerkingsverantwoordelijke heeft het recht om op zijn verzoek een audit te laten uitvoeren door een door Verwerkingsverantwoordelijke gemachtigde (rechts)persoon, ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Overeenkomst, de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet.

7.6 De kosten van de periodieke audit komen voor rekening van Verwerker. De kosten van de audit op verzoek van Verwerkingsverantwoordelijke komen voor rekening van Verwerkingsverantwoordelijke, tenzij uit de bevindingen van de audit blijkt dat Verwerker de bepalingen uit de Overeenkomst en/of de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens niet is nagekomen. Deze bepaling laat de overige rechten van Verwerkingsverantwoordelijke, waaronder het recht op schadevergoeding, onverlet.

7.7 Indien tijdens een audit wordt vastgesteld dat Verwerker niet aan het bepaalde in de Overeenkomst en/of de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet, neemt Verwerker onverwijld alle redelijkerwijs noodzakelijke maatregelen om te zorgen dat Verwerker hieraan alsnog voldoet. De bijbehorende kosten komen voor rekening van Verwerker.

De in de verwerkersovereenkomst opgenomen auditverplichting bestaat uit de volgende elementen:

1. Verwerker is verplicht periodiek een onderzoek te laten uitvoeren ten aanzien van de organisatie van verwerker, teneinde te doen vaststellen dat de leverancier voldoet aan alle in de verwerkersovereenkomst en hoofdovereenkomst opgenomen verplichtingen met betrekking tot de AVG en andere toepasselijke wet- en regelgeving op het gebied van privacy.

2. Een door de leverancier aan te wijzen onafhankelijke ICT-auditor of deskundige voert het onderzoek uit.

3. De leverancier verstrekt op verzoek van verwerkingsverantwoordelijke de resultaten van het onderzoek in de vorm van een Third Party Memorandum (TPM). Een TPM is een verklaring van een onafhankelijke externe deskundige, waarin deze een oordeel geeft over de maatregelen die een verwerker heeft getroffen in het kader van de verwerking.

4. De frequentie van het onderzoek is mede afhankelijk van een risicoclassificatie. De risicoklassen hebben betrekking op de gevoeligheid van de verwerkte persoonsgegevens.

Onderstaande tabel geeft inzicht in de risicoclassificatie van persoonsgegevens alsmede welke TPM-verplichtingen van toepassing zijn.[6]

Klasse	Persoonsgegevens	Periodiciteit
Laag	Onder deze categorie vallen gegevens waarvan algemeen aanvaard is dat deze, bij het beoogde gebruik, geen risico opleveren voor de betrokkene. Het kan hier gaan om gegevens die publiekelijk toegankelijk zijn, maar dit hoeft niet altijd het geval te zijn. Denk bijvoorbeeld aan een naam, zakelijk e-mailadres of een beroep.	Geen verplichting
Midden	Hieronder vallen persoonsgegevens die in geval van een datalek de belangen, rechten of vrijheden van de betrokkene niet in aanzienlijke mate treffen, maar die wel degelijk van belang zijn voor de betrokkene. Het gaat om persoonsgegevens die niet vallen onder de risicoklasse 'laag' of onder de categorie 'bijzondere persoonsgegevens'. Denk bijvoorbeeld aan de inschrijving van een student, financiële gegevens of locatiegegevens.	Min 2-jaarlijks
Hoog	Hieronder vallen in ieder geval persoonsgegevens die vallen in de categorie bijzondere persoonsgegevens zoals vastgelegd in de AVG (bijvoorbeeld rapporten over de psychologische gesteldheid of medische gegevens in het kader van onderzoek). Tevens vallen hier strafrechtelijke gegevens en het nationale identificatienummer (BSN/onderwijsnummer) onder.	Min jaarlijks

Uitsluitend als het gaat om persoonsgegevens met een laag risico vervalt de auditverplichting.

5. De instelling kan tussentijds om een audit verzoeken, die wordt uitgevoerd door een door de instelling gemachtigde (rechts)persoon. De kosten van de audit op verzoek komen voor rekening van de instelling, tenzij uit de bevindingen van de audit blijkt dat de leverancier de bepalingen uit de verwerkersovereenkomst niet is nagekomen. In dat geval komen de kosten voor rekening van de verwerker.
6. De kosten voor de periodieke audit komen voor rekening van de verwerker.

Bovenstaande auditverplichting is het uitgangspunt voor onderhandeling met leveranciers. Indien de praktijk het noodzakelijk maakt om af te wijken biedt het volgende hoofdstuk hierbij een handreiking.

[6] Zie het document 'Recommendations for a methodology of the assessment of severity of personal data breaches', gepubliceerd door Enisa, voor een nadere toelichting van de risicoklassen.

3. Leidraad variatie auditverplichting

3.1. Inleiding

In dit hoofdstuk wordt beschreven op basis waarvan eventueel onder voorwaarden tijdelijk kan worden afgeweken van de standaard auditverplichting indien een leverancier (nog) niet aan de auditverplichting kan voldoen.

3.2. Stap 1: Starten onderzoek naar verwerking persoonsgegevens

De eerste stap bestaat uit het vastleggen van de noodzakelijke informatie voor het bepalen van de risicoklasse, de werking van de dienst, de locatie van de gegevens en de daarmee samenhangende risico's.

Of variatie mogelijk is kan aan de hand van een set criteria worden beoordeeld. Deze criteria hebben enerzijds betrekking op de leverancier en anderzijds op de te leveren dienst. Het betreft een kwalitatieve beoordeling.

Indien er sprake is van adequate eind-tot-eind encryptie bij het aanbieden van een dienst vervalt de auditverplichting er van uitgaande dat de leverancier en/of sub verwerkers geen toegang heeft of hebben tot de persoonsgegevens en de sleutels in handen zijn van de instelling. Gezien de complexiteit en snelle ontwikkelingen met betrekking tot encryptietechnologie wordt geadviseerd dat in het geval de leverancier aangeeft dat er sprake is van eind-tot-eind encryptie onderzoek te laten plaatsvinden door materiedeskundigen.

3.2.1. Criteria voor beoordeling

Onderstaand wordt een overzicht gegeven van de criteria die relevant zijn bij de toetsing. Daarbij wordt per criterium een limitatieve set van antwoordcategorieën en een algemene toelichting gegeven.

Met betrekking tot de leverancier en de dienst worden de volgende criteria onderscheiden:

1. **De mate van inzet van sub verwerkers.**
   Toelichting: de mate van inzet van sub verwerkers alsmede het belang voor de instelling van de rol die de sub verwerkers vervullen heeft potentieel impact op het betrouwbaarheidsniveau op het vlak van de bescherming van persoonsgegevens.

   Veel sub verwerkers: er worden voor de dienst meer dan twee sub verwerkers ingezet.
   Weinig sub verwerkers / belangrijke rol: er worden voor de dienst één of twee sub verwerkers ingezet en minimaal één sub verwerker vervult bij het verwerken van persoonsgegevens een belangrijke rol (bv. een belangrijk deel of alle persoonsgegevens worden bij de sub verwerker al dan niet tijdelijk opgeslagen of onversleuteld over zijn netwerk getransporteerd).
   Weinig sub verwerkers / ondergeschikte rol: er worden voor de dienst één of twee sub verwerkers ingezet en geen van hen vervult bij het verwerken van persoonsgegevens een belangrijke rol.
   Geen sub verwerkers: er worden voor de dienst geen sub verwerkers ingezet.

2. **Het aantal betrokkenen waarvan gegevens worden verwerkt.**
   Categorieën: hoog, midden, laag.
   Toelichting: het aantal betrokkenen waarvan gegevens worden verwerkt heeft potentieel impact op de hoogte van het risico dat met de verwerking van persoonsgegevens gepaard gaat.

Hoog: de verwachting is dat binnen redelijke termijn (één jaar) na het open stellen van de dienst de persoonsgegevens van minimaal 1.000 natuurlijke personen worden verwerkt.
Midden: de verwachting is dat binnen redelijke termijn (één jaar) na het open stellen van de dienst de persoonsgegevens van minimaal 100 en maximaal 1.000 natuurlijke personen worden verwerkt.
Laag: de verwachting is dat binnen redelijke termijn (één jaar) na het open stellen van de dienst de persoonsgegevens van maximaal 100 natuurlijke personen worden verwerkt.

3. **De hoeveelheid verwerkte gegevens per betrokkene.**
   Categorieën: hoog, midden, laag.
   Toelichting: de hoeveelheid verwerkte gegevens per betrokkene heeft potentieel impact op de hoogte van het risico dat met de verwerking van persoonsgegevens gepaard gaat. Het antwoord moet gegeven worden op basis van het maximumaantal verwerkte gegevens dat redelijkerwijs een betrokkene kan betreffen. Het gaat niet om het gemiddeld aantal verwerkte gegevens. Een verwerkt gegeven moet hierbij gedefinieerd worden als een gegevenssoort. Bijvoorbeeld het gegevenssoort tentamencijfer telt als één gegevenssoort, ook al zijn er twintig tentamencijfers vastgelegd.

   Hoog: de verwachting is dat binnen redelijke termijn (één jaar) na het open stellen van de dienst van een natuurlijke persoon redelijkerwijs te verwachten meer dan 25 verschillende gegevens worden verwerkt.
   Midden: de verwachting is dat binnen redelijke termijn (één jaar) na het open stellen van de dienst van een natuurlijke persoon redelijkerwijs te verwachten meer dan 10 maar minder dan 25 verschillende gegevens worden verwerkt.
   Laag: de verwachting is dat binnen redelijke termijn (één jaar) na het open stellen van de dienst van een natuurlijke persoon redelijkerwijs te verwachten minder dan 10 verschillende gegevens worden verwerkt.

4. **Gevoeligheid van de gegevens.**
   Categorieën: bijzondere persoonsgegevens, niet bijzondere persoonsgegevens.
   Toelichting: de gevoeligheid van de verwerkte gegevens heeft potentieel impact op de hoogte van het risico dat met de verwerking van persoonsgegevens gepaard gaat. Het gaat hierbij om de gevoeligheid van het verwerkte gegeven dat als het meest gevoelig kan worden gekwalificeerd. Het gaat niet om de gemiddelde gevoeligheid. Wat gevoelige gegevens zijn is omschreven in de AVG als bijzondere persoonsgegevens.

   Bijzondere persoonsgegevens: gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische of biometrische gegevens met het oog op de unieke identificatie van een persoon, gegevens over gezondheid, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid. Tevens vallen strafrechtelijke gegevens en het nationale identificatienummer (BSN) hieronder.
   Niet bijzondere persoonsgegevens: persoonsgegevens niet zijnde bijzondere persoonsgegevens.

5. **Impact voor betrokkene.**
   Categorieën: hoog, midden, laag.
   Toelichting: de impact die de verwerking van persoonsgegevens voor de betrokkene kan hebben heeft potentieel impact op de hoogte van het risico dat met de verwerking van persoonsgegevens gepaard gaat. Het gaat hierbij om de maximale impact dat het gevolg van de verwerking kan zijn. Het gaat niet om de gemiddelde impact.

Hoog: de impact die de verwerking van persoonsgegevens voor de betrokkene kan hebben kan als hoog worden gekwalificeerd. Hierbij valt te denken aan maatregelen waaraan voor de betrokkene rechtsgevolgen zijn verbonden of die de belangen, rechten of vrijheden van de betrokkene in aanzienlijke mate treffen.
Bijvoorbeeld het verkrijgen van diploma's, leningen, gezondheidsbehandeling e.d.
Midden: de impact die de verwerking van persoonsgegevens voor de betrokkene kan hebben kan als midden worden gekwalificeerd. Hierbij valt te denken aan maatregelen waaraan voor de betrokkene geen rechtsgevolgen zijn verbonden of die de belangen, rechten of vrijheden van de betrokkene niet in aanzienlijke mate treffen, maar die wel degelijk van belang zijn voor de betrokkene.
Bijvoorbeeld het verkrijgen van toegang tot studiemateriaal.
Laag: de impact die de verwerking van persoonsgegevens voor de betrokkene kan hebben kan als laag worden gekwalificeerd.
Bijvoorbeeld het verkrijgen van de mogelijkheid om tegen gunstige prijzen software aan te schaffen.

6. **Locatie van de persoonsgegevens.**
   Categorieën: buiten EER / wel één van de in de AVG genoemde voorwaarden voor doorgifte naar derde landen (artikel 45, 46, 47 en 49), binnen EER, binnen NL.
   Toelichting: de locatie van de persoonsgegevens heeft potentieel impact op de hoogte van het risico dat met de verwerking van persoonsgegevens gepaard gaat. Indien de locatie dynamisch is, dat wil zeggen dat de exacte locatie niet kan worden bepaald, dan moet gekozen worden voor de eerst mogelijke categorie. Ditzelfde principe geldt ook als de locatie van de persoonsgegevens wisselt per soort persoonsgegeven.

   Buiten EER / wel een van de in de AVG genoemde voorwaarden voor doorgifte naar derde landen: de locatie van de persoonsgegevens ligt buiten de Europese Economische Ruimte (EU-landen aangevuld met Noorwegen, Liechtenstein en IJsland), maar er is wel sprake van een adequaat beschermingsniveau, passende waarborgen of een van de uitzonderingen uit artikel 49 AVG.
   Leveranciers uit de VS kunnen zich certificeren voor het Privacy Shield en als zij zich hebben gecertificeerd bieden zij een 'adequaat beschermingsniveau'.
   Binnen EER: de locatie van de persoonsgegevens ligt binnen de Europese Economische Ruimte (EU-landen aangevuld met Noorwegen, Liechtenstein en IJsland).
   Binnen NL: de locatie van de persoonsgegevens ligt binnen Nederland.

Indien gewenst kunnen aanvullende criteria worden gebruikt zoals: trackrecord van de leverancier, innovatieve dienst etc.

3.2.2. Stap: vaststellen knock-out

De eerste deelstap bij een beoordeling is het vaststellen of er sprake is van een zogenaamde “knock-out” waarbij variatie op de auditverplichting sowieso niet wenselijk is. Onderstaand overzicht geeft een opsomming van de knock-out’s

Criterium	Knock-out
Gevoeligheid gegevens	Bijzondere persoonsgegevens
Impact voor betrokkene	Hoog

Indien één knock-out van toepassing is, is afwijken van de auditverplichting niet wenselijk.

3.2.3. Stap: beoordeling aan de hand van de criteria

Indien er geen knock-out van toepassing is wordt vervolgd met een kwalitatieve waardering met betrekking aan de hand van de genoemde criteria. Het is van belang om de criteria in onderlinge samenhang te wegen. Aan de hand van de kwalitatieve beoordeling kan verder worden nagedacht over de variatie.

3.3. Stap 2: mogelijke variatie op auditverplichting

Onderstaand wordt eerst inzicht gegeven in de variatiemogelijkheden op de auditverplichting:

1. Een tijdelijk uitgestelde verplichting, inclusief compenserende maatregelen. Er wordt geadviseerd een termijn van 6 of maximaal 12 maanden te hanteren en dit op te nemen in de verwerkersovereenkomst. Een compenserende maatregel kan een door de instelling geaccordeerde beschrijving over de opzet van de beveiliging zijn.

2. Een andere uitvoerder van het onderzoek (in plaats van de externe ICT-auditor in opdracht van de leverancier):

   - Een externe ICT-auditor of deskundige (in opdracht) van de instelling.
   - Eén of meerdere instellingen in opdracht van de leverancier.
   - Eén of meerdere instellingen in opdracht van één of meerdere andere instellingen (peer audit).
   - Self-assessment van een instelling op basis van SURFaudit.

3. Een ander Normenkader voor het onderzoek:
   - Specifieke benoemde normenkaders (bv. Zorg Service Provider, SURFaudit).
   - Specifiek benoemde Best Practice bepalingen.

4. Het niet verrichten van een onderzoek naar de werking van de onderzochte maatregelen, maar uitsluitend naar opzet en bestaan.

Het is belangrijk om de voorgestelde variatie op de auditverplichting uitdrukkelijk te onderbouwen en vergezeld te laten gaan met de te treffen compenserende maatregelen.