Gebruiksvoorwaarden logo Privacy Audit Proof

Inleiding

In de markt bestaat een expliciete behoefte om zichtbaar te maken dat maatregelen voor het borgen van privacy zijn genomen. Om aan deze behoefte te kunnen voldoen, is binnen NOREA, de beroepsorganisatie van IT-auditors in Nederland, het logo Privacy Audit Proof ontwikkeld.

Het logo Privacy Audit Proof is een door de NOREA gedeponeerd woord- en beeldmerk. NOREA beschikt over alle rechten met betrekking tot dit logo, dat kan worden gebruikt ten behoeve van Privacy Audit Proof. In deze gebruiksvoorwaarden zijn de voorwaarden voor het toekennen en gebruik van het logo uitgewerkt. Organisaties dienen hieraan te voldoen voor het voeren van het logo.

NOREA zorgt voor de randvoorwaarden en regelgeving met betrekking tot assurance-opdrachten, maar controleert of verifieert niet onafhankelijk de naleving van de richtlijnen door al degenen (bedrijven en instellingen) die het logo gebruiken, noch geeft de vertoning van het logo aan dat er geen tekortkomingen of uitzonderingen bij de uitvoering van de betrokken opdrachten zijn vastgesteld.

NOREA kan geen uitdrukkelijke of impliciete verklaringen of garanties geven met betrekking tot partijen die één of meerdere van haar logo's vertonen. De verantwoordelijkheid voor uitvoering van assurance-opdrachten en de daarmee gekoppelde logo's ligt altijd bij de IT-auditor of de organisatie waarbij hij of zij werkzaam is.

1. Definities

Algemene Verordening Gegevensbescherming (AVG): Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van gegevens en tot intrekking van Richtlijn 95/ 46/ EG.

Assurance-rapport: rapport als bedoeld in NOREA-Richtlijn 3000A met het NOREA Privacy Control Framework (PCF) als normenkader of conform de handreiking voor het opstellen van SOC2 en SOC3 assurance-rapporten waarbij de privacy-categorie in scope is. Zie verder de Handreiking, waar de assurance-rapporten als resultaat van de privacy-audits verder zijn beschreven en relevante templates zijn opgenomen.

Logo: het bij het Benelux Merkenbureau geregistreerde woord- en beeldmerk Privacy Audit Proof.

NOREA: de beroepsorganisatie van IT-auditors.

Aanvrager: degene die is bevoegd tot het verstrekken van de opdracht tot het uitvoeren van een privacy-audit en deze opdracht ook daadwerkelijk verstrekt.

Privacy-audit: de werkzaamheden die in het kader van een assurance-rapport door een privacy-auditor worden uitgevoerd teneinde na te gaan in hoeverre het stelsel van maatregelen en procedures gericht op de bescherming van persoonsgegevens in opzet en bestaan dan wel opzet, bestaan en werking aanwezig is. Zie de Handreiking, waar de voorwaarden voor het uitvoeren van privacy-audits verder zijn uitgewerkt.

Privacy-auditor: de Register IT-auditor (RE), die beschikt over de vereiste deskundigheid op het gebied van privacy, zoals bedoeld in artikel 130 van het Reglement Gedragscode.

Privacy Control Framework (PCF): Het door NOREA opgestelde overzicht van beheersingsdoelstellingen en beheersingsmaatregelen voor de uitvoering van privacy-audits en privacy-assurance-opdrachten.

Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens. Bij het verwerken moet sprake zijn van een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel.

Verwerkingsverantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel en de middelen voor de verwerking van persoonsgegevens vaststelt, zoals bedoeld in artikel 30 van de AVG.

Verwerker: een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

2. Eigendom logo Privacy Audit Proof

2.1 NOREA is eigenaar van het logo Privacy Audit Proof.

2.2 De aanvrager van het logo, zal bij de aanvraag NOREA vrijwaren van alle aanspraken van derden inzake het (oneigenlijk) gebruik van het logo.

3. Voorwaarden voor toekenning logo Privacy Audit Proof

3.1 Het logo Privacy Audit Proof kan zowel aan een verwerkingsverantwoordelijke als een verwerker worden toegekend.

3.2 Voor het verkrijgen van het logo Privacy Audit Proof dient de aanvrager verwerkingsverantwoordelijke dan wel verwerker te zijn en te beschikken over een assurance-rapport met een positief oordeel zonder beperkingen, gebaseerd op een privacy-audit gericht op het verkrijgen van "redelijke mate van zekerheid" over privacy-beheersing.

3.3 De privacy-audit dient te worden uitgevoerd door een privacy-auditor conform de assurance-richtlijn Richtlijn 3000A en in geval van SOC-rapporten de basis zijn, de handreiking voor het opstellen van SOC2 en SOC3 assurance-rapporten, waarbij de privacy-categorie in scope is.

3.4 Voor het initieel aanvragen van het logo is, in geval toepassing van de assurance-richtlijn 3000A, een onderzoek naar opzet en bestaan voldoende. Voor de daaropvolgende verleningen van het logo dient een assurance-onderzoek naar opzet, bestaan en werking over de periode van een jaar te worden uitgevoerd. Bij aanvraag op basis van SOC3-assurance-rapport, dient in lijn met de van toepassing zijnde Handreiking, in alle gevallen een onderzoek naar opzet, bestaan en werking worden uitgevoerd.

3.5 Het assurance-rapport kan betrekking hebben op een totale verwerking of een deel daarvan, of een aantal verwerkingen, in geval van een verwerkingsrelatie.

3.6 Het assurance-onderzoek dient alle beheersingsdoelstellingen uit het PCF te omvatten die relevant zijn voor de verwerkingsverantwoordelijke dan wel verwerker. Daar waar relevant, kunnen aanvullende beheersingsdoelstellingen uit bijvoorbeeld relevante sectorale wetgeving aan het NOREA PCF te worden toegevoegd.

3.7 De maatregelen opgenomen in het PCF zijn *illustratieve* maatregelen. De aanvrager dient aan de privacy-auditor aan te tonen welke maatregelen hij/ zij heeft genomen voor elk van de opgenomen beheersingsdoelstellingen. Als de aanvrager andere "frameworks" dan het NOREA PCF hanteert, dient hij/ zij bij de aanvraag een kruisreferentie naar de NOREA PCF beheersingsdoelstellingen aan de auditor aan te leveren.

3.8 Het assurance-rapport dient te zijn voorzien van een ondertekende managementverklaring. Bij de long form assurance rapport wordt ook het beheersingsraamwerk inclusief testwerkzaamheden en resultaten. Een systeembeschrijving is verplicht als onderdeel van het SOC2- en SOC3-rapport.

3.9 In de bijlagen bij deze handreiking zijn (minimale) templates opgenomen voor de long form en short form assurance-rapportage en de SOC3-rapportage:

- De long form rapportage is de rapportage die standaard wordt opgesteld door de privacy-auditor in het kader van een "privacy assurance" dan wel "Privacy audit Proof opdracht". De long form rapportage wordt uitgegeven richting de klant om een oordeel te geven over privacy beheersingsmaatregelen.

- Bij een schone verklaring (zonder bevindingen) kan een *short form* rapportage worden opgesteld. De short form rapportage is bedoeld voor brede verspreiding/publicatie ter onderbouwing van het logo Privacy Audit Proof.
- De SOC3 rapportage kan worden opgesteld in geval van een "schone" SOC2 verklaring (goedkeurend oordeel), waarbij het NOREA PCF is gebruikt voor invulling van de privacy criteria.

4. Het aanvragen van het logo

4.1 De aanvrager kan aan NOREA het logo Privacy Audit Proof vragen, nadat de privacy-audit met een positief oordeel, zonder beperkingen is afgerond, relevante gegevens aan de NOREA zijn verstrekt en is voldaan aan de voorwaarden, zoals onder 3 beschreven.

4.2 Voor aanvraag van het Privacy Audit Proof logo via de website van NOREA dient de short form dan wel de SOC3-rapportage te worden meegestuurd/geüpload ter onderbouwing van de aanvraag van het logo Privacy Audit Proof.

4.3 NOREA houdt administratie bij van aanvragen, de onderbouwing en het toekennen van het logo.

5. Gebruiksvoorwaarden logo

5.1 Het logo mag kan worden toegepast op de website in brochures en overige uitingen van de aanvrager.

5.2 Het logo mag alleen worden gebruikt in vorm waarin het is verkregen en mag alleen worden aangepast voor wat betreft de grootte.

5.3 De toestemming voor het gebruik van het logo wordt door NOREA verleend aan de aanvrager voor een periode van twaalf (12) maanden en kan worden verlengd, indien binnen zestig (60) dagen na afloop van de twaalf (12) maands-periode opnieuw op vergelijkbare wijze een assurance-rapport met een positief oordeel zonder beperkingen gericht op het verkrijgen van een "redelijke mate van zekerheid" met betrekking tot dezelfde verwerkingsactiviteiten van de aanvrager is afgegeven en aan NOREA wordt verstrekt.

5.4 De verleende toestemming tot het gebruik van het logo kan door de privacy-auditor op basis van professionele oordeelsvorming (tijdelijk) worden ingetrokken.

5.5 De aanvrager van het logo, verplicht zich tot:

- Het in stand houden en laten functioneren van het stelsel van maatregelen en procedures gericht op de verwerking, zoals aangegeven in het assurance-rapport;
- Het actief melden aan de privacy-auditor, gedurende de periode waarin het logo mag worden gebruikt, van alle relevante wijzigingen en onrechtmatigheden in de verwerking

van persoonsgegevens en het stelsel van maatregelen en procedures. Het gaat hierbij onder andere om eigen meldingen van datalekken en uitingen van de Autoriteit Persoonsgegevens (AP) over de beoordeelde verwerking van persoonsgegevens;

- Het binnen zestig (60) dagen verwijderen van het logo nadat de geldigheidstermijn is verstreken, ofwel op aangeven van de NOREA, ofwel het logo door de privacy-auditor tijdelijk is ingetrokken of definitief is beëindigd. Zie verder artikel 5.

5.6 Het assurance-rapport, waarop het logo is gebaseerd, dient direct, zonder beperkingen, zoals “hold harmless letter” of gebaseerd op verspreidingskring, opvraagbaar te zijn.

6 Tijdelijke intrekking en definitieve beëindiging logo

6.1 De verleende toestemming tot het gebruik van het logo kan door de privacy-auditor op basis van professionele oordeelsvorming tijdelijk worden opgeschort of definitief worden ingetrokken indien bijvoorbeeld:

- door de privacy-auditor wordt vastgesteld dat de aanvrager enige verplichting als opgenomen in deze gebruiksvoorwaarden niet naleeft en/of;
- tijdens een controle na het toekennen van het logo door de privacy-auditor tekortkomingen worden geconstateerd, die afbreuk doen aan het reeds afgegeven positieve oordeel en/of;
- de privacy-auditor niet de door hem/ haar noodzakelijke geachte onderzoekwerkzaamheden kan uitvoeren voor het opheffen van intrekking van het logo.

6.2 De verleende toestemming tot het gebruik van het logo eindigt als de houder van het logo (verwerkingsverantwoordelijke of verwerker) niet binnen zestig (60) dagen na de geldigheidsduur van het logo een door NOREA afgegeven verlenging kan overleggen.

7 Kwaliteitsborging en afhandeling klachten

7.1 De NOREA bewaakt de kwaliteit van privacy-audits, als onderdeel van reguliere kwaliteitsonderzoeken.

7.2 Eventuele vragen, opmerkingen of klachten worden via de standaardprocedures van de NOREA afgehandeld.

Bijlagen:

- I. Template long form assurance-rapportage
- II. Template short form assurance-rapportage
- III. Template SOC3-rapportage