Privacy-Audit (Proof)

DUIJNBORGH AUDIT®

Waarom een Privacy-audit?

Organisaties die persoonsgegevens verwerken moeten verschillende beheersmaatregelen opzetten en implementeren om te zorgen dat de verwerking binnen de kaders van de wetgeving plaatsvindt. Sinds de (formele) invoering van de AVG in mei 2018, zijn de regels verscherpt. Als persoonsgegevens worden verwerkt, dan moeten deze gegevens op een adequate wijze worden beschermd en beveiligd. De AVG spreekt over “passende technische en organisatorische maatregelen, rekening houdend met de stand van de techniek”.

Om hier concrete invulling aan te geven en organisaties in staat te stellen om te bepalen aan welke eisen moet worden voldaan, hoe persoonsgegevens moeten worden beschermd en wanneer maatregelen passend en redelijk zijn, heeft de NOREA (de Nederlandse organisatie van Register EDP-auditors) het Privacy Control Framework (PCF) uitgebracht. Het PCF is ontwikkeld voor geregistreerde IT-auditors (Register IT-auditors, RE’s) om hen te ondersteunen bij het doen van onderzoek naar de compliancy inzake de AVG.

Duijnborgh Audit voert privacy-audits uit aan de hand van het PCF en certificeert organisaties zodat zij het Keurmerk Privacy Audit Proof mogen voeren.

Wat levert een privacy-audit voor u op?

- Allereerst kunt u met behulp van de uitkomsten van de privacy-audit verbeteringen aanbrengen en daarmee zorgen dat uw organisatie persoonsgegevens binnen de kaders van de wet verwerkt.
- Daarnaast kunt u aan uw klanten laten zien (bijvoorbeeld middels het Privacy Audit Proof keurmerk) dat de persoonsgegevens die betrokkenen, klanten of opdrachtgevers met u delen of aan u verstrekken, bij u in goede handen zijn.
- Een goede bescherming van persoonsgegevens is in veel gevallen een belangrijk criterium bij de gunning van opdrachten. Met een privacy-audit heeft u een ‘voorsprong’ ten opzichte van partijen die dit niet kunnen aantonen.
- Tot slot kunt u, in voorkomend geval -bijvoorbeeld na een incident-, aan de toezichthouders (o.a. de Autoriteit Persoonsgegevens) aantonen dat uw organisatie er alles aan gedaan heeft om inbreuken op de bescherming van persoonsgegevens te voorkomen.

Waarom Duijnborgh Audit?

Duijnborgh Audit is gespecialiseerd op het (brede) gebied van IT-auditing. Onze medewerkers zijn gekwalificeerde IT-auditors en door ons lidmaatschap van de NOREA zijn onze klanten verzekerd van een onafhankelijke beoordeling.

Wij zien audits niet zozeer als ‘beoordeling van…’ maar meer als instrument voor organisaties om in te zetten ter verbetering van de processen. Wij streven met onze aanpak een betrouwbare en integere informatievoorziening na.

PRIVACY audit proof

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Gefaseerde aanpak

Onze aanpak is erop gericht het Privacy Audit Proof Keurmerk in twee stappen aan uw organisatie te verstrekken.

1. Start

Bij de start zullen we met uw organisatie vaststellen wat de scope dient te zijn van de privacy-audit en wat de gewenste planning is.

2. Risicoprofiel en beheersingsdoelstellingen opstellen

In deze stappen brengen we samen met uw organisatie de risico's in beeld die betrekking hebben op verwerking van persoonsgegevens in uw organisatie. Op basis van de risico's kunnen we vervolgens gezamenlijk vaststellen wat de noodzakelijke beheersingsdoelstellingen en -maatregelen zijn. We gebruiken hiervoor als basis het Privacy Control Framework van de NOREA.

3. Pre-audit en terugkoppeling

De beheersmaatregelen worden in opzet, bestaan en werking in een korte tijd gecontroleerd om een eerste indruk te verkrijgen. De bevindingen worden aan u teruggekoppeld. Op basis van de uitkomsten van de pre-audit wordt tevens vastgesteld wanneer stap 5 kan starten.

4. Iteratief proces verbeteracties

Op basis van de uitkomsten van de pre-audit brengt uw organisatie gewenste verbeteringen aan. Duijnborgh Audit is gedurende deze periode –en waar dat binnen haar auditrol past- beschikbaar voor het tussentijds beoordelen van de verbeteracties. Hierdoor worden verrassingen achteraf voorkomen en wordt de kans van slagen bij de eindbeoordeling aanzienlijk vergroot.

5. Audit opzet en bestaan

Op het moment dat uw organisatie aangeeft dat zij klaar is met de implementatie van de gewenste beheersmaatregelen, zullen wij een onderzoek uitvoeren ter beoordeling van de opzet en het bestaan. Ervan uitgaande dat alle daarvoor bekende en gerapporteerde tekortkomingen zijn verholpen en dat alle noodzakelijke beheersmaatregelen zijn geïmplementeerd, wordt de audit afgerond met de afgifte van een rapport waarin Duijnborgh Audit een verklaring afgeeft over de geschiktheid van het ontwerp en de implementatie van noodzakelijke beheersmaatregelen (naar de stand van dat moment).

6. Keurmerk 'Privacy Audit Proof'

Op voorwaarde dat het oordeel 'met redelijke mate van zekerheid en zonder beperking in het oordeel' is, dragen wij uw organisatie bij de NOREA voor om het Keurmerk Privacy Audit Proof te verkrijgen. Tevens stellen wij een (papieren en digitaal) certificaat op met een geldigheid van 1 jaar. Uw Keurmerk wordt gepubliceerd op de website (www.privacy-audit-proof.nl) en u bent, zolang het certificaat geldig is, gerechtigd op uw website en andere publicaties het logo van Privacy-Audit-Proof te gebruiken.

7. Audit effectieve werking (tweede en volgende jaren)

(Ruim) voor de afloopdatum van het certificaat zullen wij contact met u opnemen voor de verlenging van het certificaat. Vanaf het tweede jaar zullen wij naast de 'opzet' en het 'bestaan' ook de 'werking' toetsen. Dat wil zeggen dat wij toetsen of gedurende de afgelopen periode de gewenste beheersmaatregelen effectief hebben gewerkt.

Duijnborgh Audit BV
Papendorpseweg 100
3528 BJ Utrecht
T 31(0)88 - 1601700
F 31(0)88 - 1601799
E info@dbaudit.nl

DUIJNBORGH AUDIT®