NOREA WEBINAR: PRIVACY PRODUCTEN – 17 juni, 19.00 uur

- Het NOREA Privacy Control Framework (PCF 2.0) en AVG-certificering door Ed Ridderbeekx
- De NOREA Data Protection Impact Assessment (DPIA 2.0) door Jeroen van Puijenbroek en Henk van der Linde
- Het vernieuwde logo Privacy Audit Proof op basis van Richtlijn 3000 of SOC2/3 door Henk Hendriks en Maurice Koetsier

NOREA
Privacy Control Framework
(en AVG certificering)

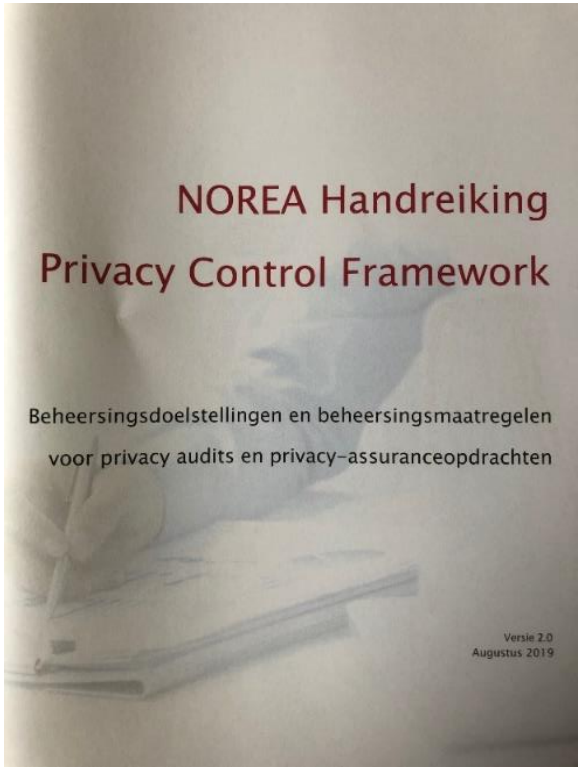
Ed Ridderbeekx

Webinar Privacy,17 juni 2021

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Er was behoefte aan een “Privacy Control Framework”

- AVG, actualiteit en marktvraag
- Guidance bij implementatie én auditing
- Aantoonbaarheid beheersing
- Onderscheidend vermogen



PCF - Doelstelling en gebruikers

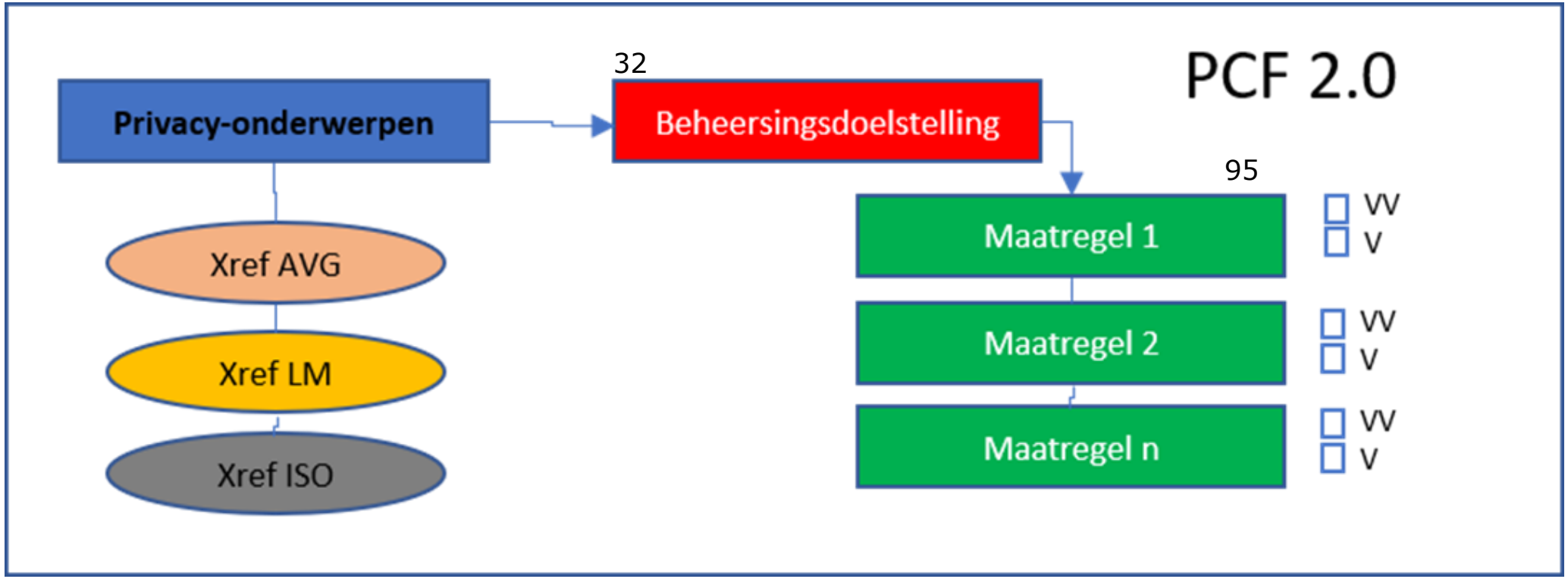
Doel:

Het bieden van ondersteuning aan (audit)professionals bij de beoordeling of de beheersingsdoelstellingen van een entiteit met betrekking tot privacy en bescherming van persoonsgegevens worden behaald.

Gebruik(ers):

- IT–auditors in (privacy–) audits
- IT– auditors in assurance opdrachten
- IT–auditors ihkv Privacy Audit Proof™–logo
- Andere professionals

PCF – Structuur



Voorbeeld: Beheersingsdoelstelling & maatregelen

Data protection impact assessments (PIA)		
Beheersingsdoelstelling: De privacy-gerelateerde effecten van nieuwe producten en diensten en het gebruik ervan binnen de entiteit worden op systematische wijze geïdentificeerd, beoordeeld en aangepakt.		
Fase informatielevenscyclusmanagement: **Management**		
Beheersingsmaatregelen:		*Bevindingen/ toetsing:*
PIA01	De entiteit beoordeelt aan de hand van een gedocumenteerd proces de effecten op privacybescherming van nieuwe of sterk gewijzigde processen, producten en diensten (DPIA).	VV
PIA02	Bij de DPIA wordt vastgesteld: a. de aard van de geplande verwerkingen; b. hun doelstelling, noodzaak, en proportionaliteit; c. de privacyrisico's die beoogde verwerkingen met zich meebrengen voor betrokkenen; d. welke maatregelen moeten worden genomen om deze risico's te beperken.	VV
~~PIA03~~	*Samengevoegd met PIA02.*	
PIA04	Alle relevante belanghebbenden zijn bij de DPIA betrokken en de specifieke richtlijnen van de toezichthoudende autoriteit ten aanzien van beoordelingscriteria worden nageleefd.	VV
PIA05	De entiteit documenteert welke systemen en software persoonsgegevens verwerken en houdt bij welke wijzigingen hierin zijn doorgevoerd.	VV
PIA06	Een verandermanagementproces is vastgesteld om ervoor zorg te dragen dat de in de DPIA goedgekeurde privacymaatregelen zijn geïmplementeerd voordat de wijziging wordt doorgevoerd.	VV
Gerelateerde kernelementen van de AVG: • Gegevensbeschermingseffectbeoordeling		

BHD PIA:

De privacy–gerelateerde effecten van nieuwe producten en diensten en het gebruik ervan binnen de entiteit worden op systematische wijze geïdentificeerd, beoordeeld en aangepakt.

BHM PIA01

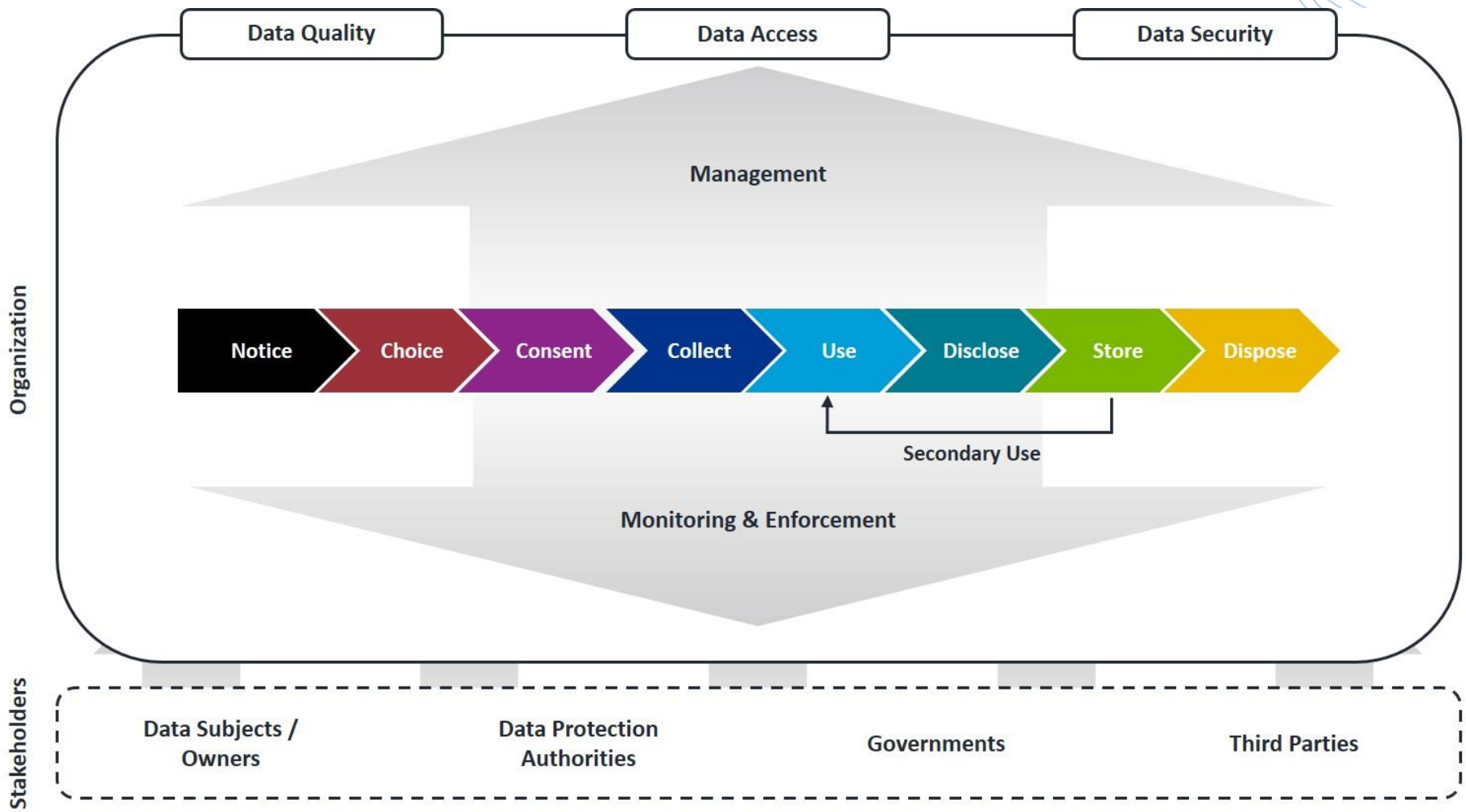
De entiteit beoordeelt aan de hand van een gedocumenteerd proces de effecten op privacybescherming van nieuwe of sterk gewijzigde processen, producten en diensten (DPIA).

PCF - aansluiting met artikelen uit de AVG

- De aansluiting met kernelementen van de AVG is geborgd (zie Annex 1– PCF)

GDPR key element	GDPR article(s)
Privacy Principles	5
Lawfulness of Processing	6
Conditions for Consent	7
Rights of the data subject	12-19
Right to data portability	20
Privacy By Design / by Default	25
Responsibilities of controller and processor	24, 28
Records of processing activities	30
Security of processing	32
Personal Data Breach	33, 34
Data Protection Impact Assessment (DPIA)	35
Data Protection Officer (DPO)	37-39
Transfers of personal data to third countries or international organisations	44-50

Informatielevenscyclusmodel (ILM) als uitgangspunt



PCF: wijzigingen in versie 2.0

- Verbetering en aanscherping formulering doelstellingen en maatregelen
- Aantal maatregelen van 104 naar 95
- Indicatie maatregelen van toepassing op verwerkingsverantwoordelijke/ verwerker/beide
- Verduidelijking relatie met andere privacy-instrumenten NOREA (zoals *Privacy Audit Proof*)
- Relatie/x-ref met ISO-standaarden (27001, 27701)
- Nederlandse én Engelse versie (zie www.norea.nl)

Toepassing PCF

- Neem een risk based approach
- Stem gebruik PCF af op specifieke (privacy–)omstandigheden van een organisatie
- Toepassing PCF garandeert geen AVG compliance
- (Laat ons je feedback weten)

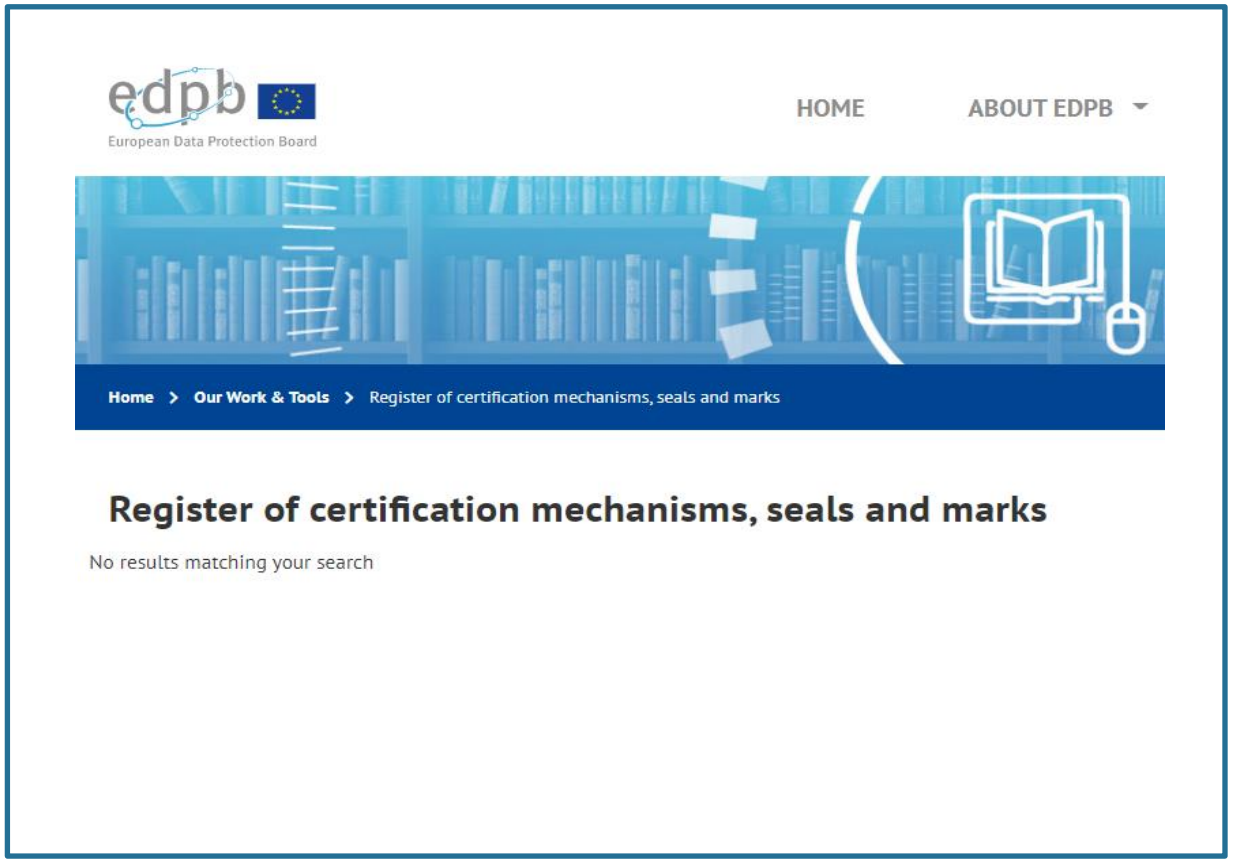
AVG Certificering – een verwarrend landschap

	Audit	Assurance	Certificering*	Logo/Keurmerk
NOREA's PCF	✓	✓	??	✓

** In de betekenis van art. 42 en 43 AVG*

"The Member States, the supervisory authorities, the [European Data Protection] Board and the European Commission shall encourage, in particular at the Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors. (…)".

Stand van zaken



AUTORITEIT
PERSOONSGEGEVENS

AVG-certificaat aanvragen

Organisaties kunnen op termijn een AVG-certificaat aanvragen bij een certificatie-instelling die is goedgekeurd (geaccrediteerd) door de Raad voor accreditatie (RvA). Op dit moment zijn er in Nederland nog geen certificatie-instellingen geaccrediteerd voor het afgeven van AVG-certificaten. Zodra de RvA certificatie-instellingen heeft geaccrediteerd, is dat te lezen op de website van de AP en die van de RvA.

Accreditatie en certificering

Richtlijnen voor accreditatie van certificerende instellingen

Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR.

Richtlijnen voor certificering en certificeringscriteria

- Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation.
- Guidance – Addendum (Annex to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation) (consultation)

Ondertussen…

- Ongeaccrediteerde certificaten
- Certificeren tegen een gedragscode: NL Digital's *Data Pro Code*
- ISO 27701 als 'privacy add-on' op ISO 27001 (PIMS)
- Privacy Control Framework?

Vragen?

NOREA WEBINAR: PRIVACY PRODUCTEN - DPIA 2.0

DPIA – Wat is het?

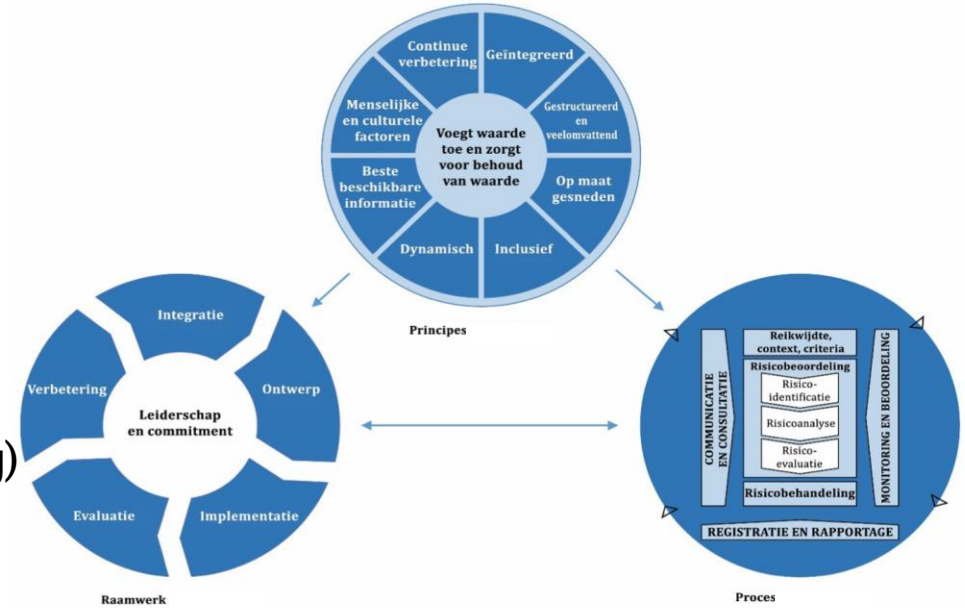
- "Een instrument om vooraf de privacyrisico's van een verwerking van persoonsgegevens in kaart te brengen, en om daarna maatregelen te kunnen nemen om de risico's te verkleinen." (AP);
- "Een goed uitgevoerde DPIA geeft inzicht in de *risico's die de verwerking oplevert voor de betrokkenen*, en in de *maatregelen die de verantwoordelijke moet nemen* om de risico's af te dekken." (AP);
- Artikel 35 (7) AVG.

I. Beschrijving gegevensverwerking	II. Beoordeling rechtmatigheid	III. Risicobeoordeling en -behandeling

NOREA WEBINAR: PRIVACY PRODUCTEN - DPIA 2.0

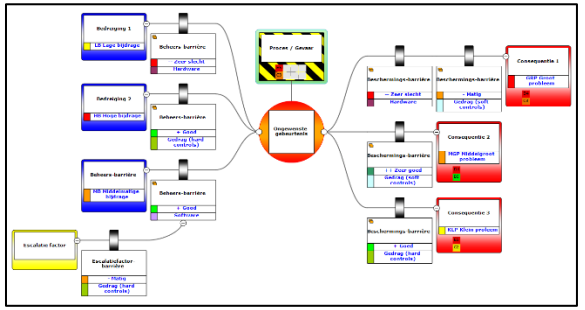
Twee producten:

1. NOREA Handreiking DPIA
   - Introductie en proces (wat, waarom, wanneer, wie, …)
   - Toelichting op de vragen uit het DPIA Raamwerk
   - Bijlagen (o.a. criteria verplichte DPIA en vb–en risicobeoordeling)
2. NOREA DPIA Raamwerk
   - De te beantwoorden vragen in de DPIA…
   - …die na beantwoording leiden tot de DPIA–rapportage



NOREA WEBINAR: PRIVACY PRODUCTEN - DPIA 2.0

Structuur



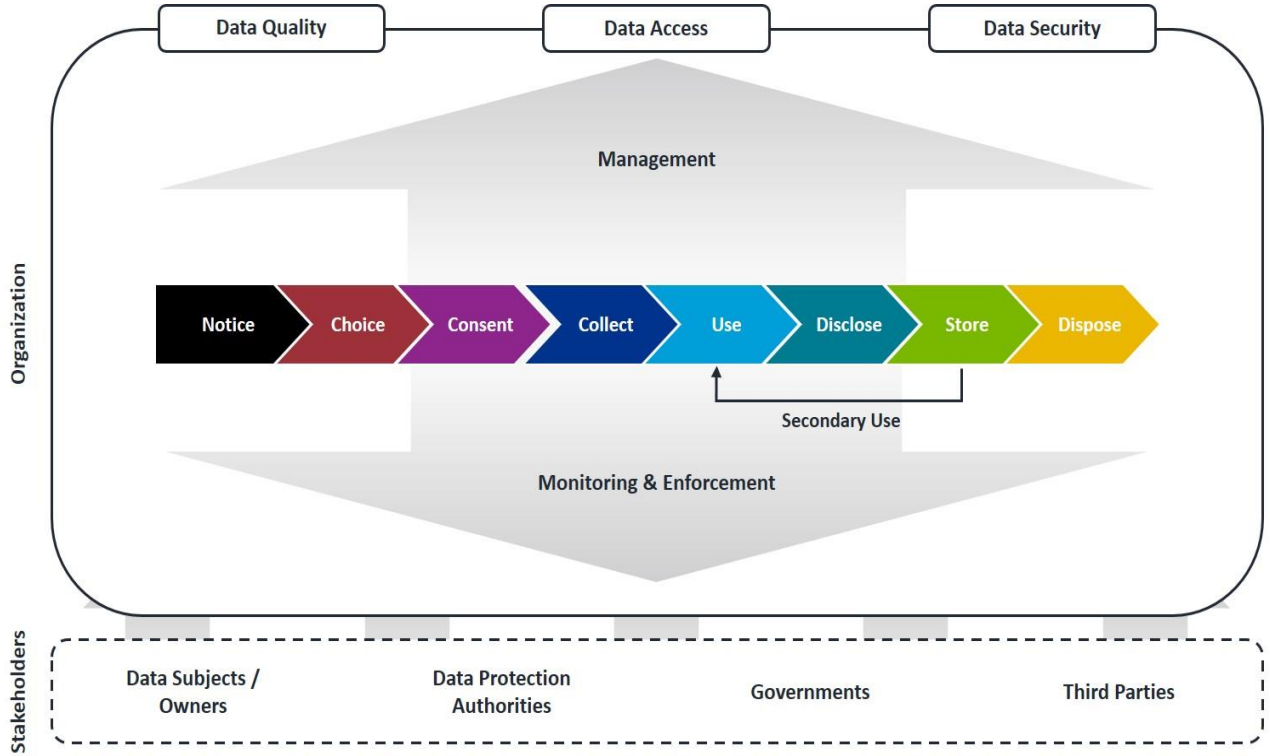
NOREA WEBINAR: PRIVACY PRODUCTEN - DPIA 2.0

Structuur

NOREA WEBINAR: PRIVACY PRODUCTEN – DPIA 2.0

Raamwerk

1. **Beschrijving gegevensverwerking**
   - **Contextanalyse DPIA:**
     - Beschrijving hoofdlijnen project
     - Doelen van en eisen aan project
     - Beschrijf relevante bedrijfsprocessen en gegevensstromen;
     - Gerelateerde IT–systemen en/of interfaces naar andere platforms
     - Beschrijf van toepassing zijn de wetgeving(en);



NOREA WEBINAR: PRIVACY PRODUCTEN - DPIA 2.0

Structuur

Raamwerk: 2. Rechtmatigheidsbeoordeling

- Grondslag:
  - Toestemming
  - Overeenkomst
  - Wettelijke verplichting
  - Vitaal belang
  - Taak algemeen belang
  - Gerechtvaardigd belang
- Noodzaak en evenredigheid
- Uitoefening rechten betrokkene

Zorg
Wabvpz
WGBO
Financieel
Wft
Pensioen
Wwft

Gemeenten
Jeugdwet
WMO
Schuldhulp

Handhaving
Wpg
Ondermijning

lex specialis derogat legi generali

Indien 'Wettelijke Verplichting' of 'Taak Algemeen Belang':

- "Lex specialis versus lex generalis", wet stelt Sectorale wetgeving boven Algemene wetgeving;
- Let ook op specifieke Sectorale standaarden.

NOREA WEBINAR: PRIVACY PRODUCTEN - DPIA 2.0

Structuur

Handreiking DPIA

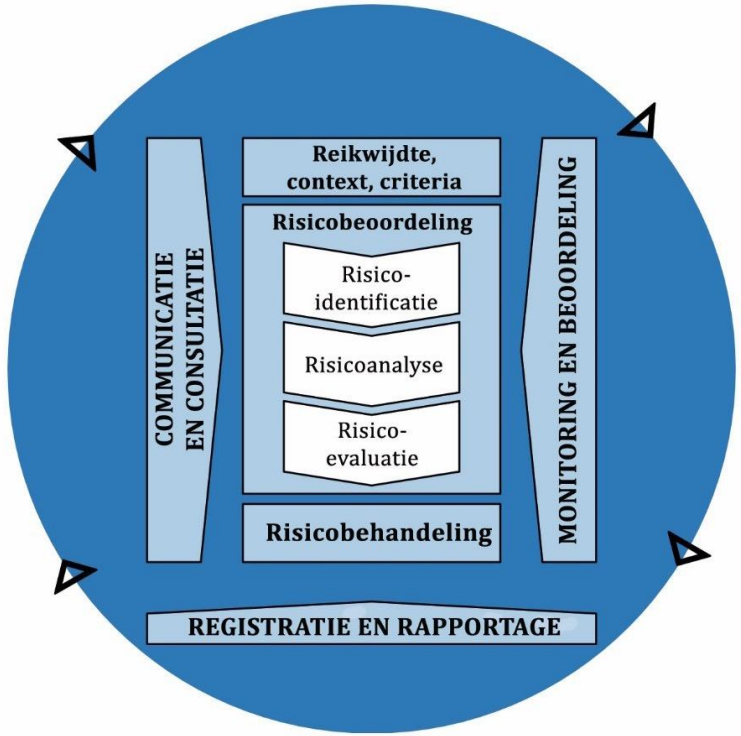
I. Beschrijving gegevensverwerking

II. Beoordeling rechtmatigheid

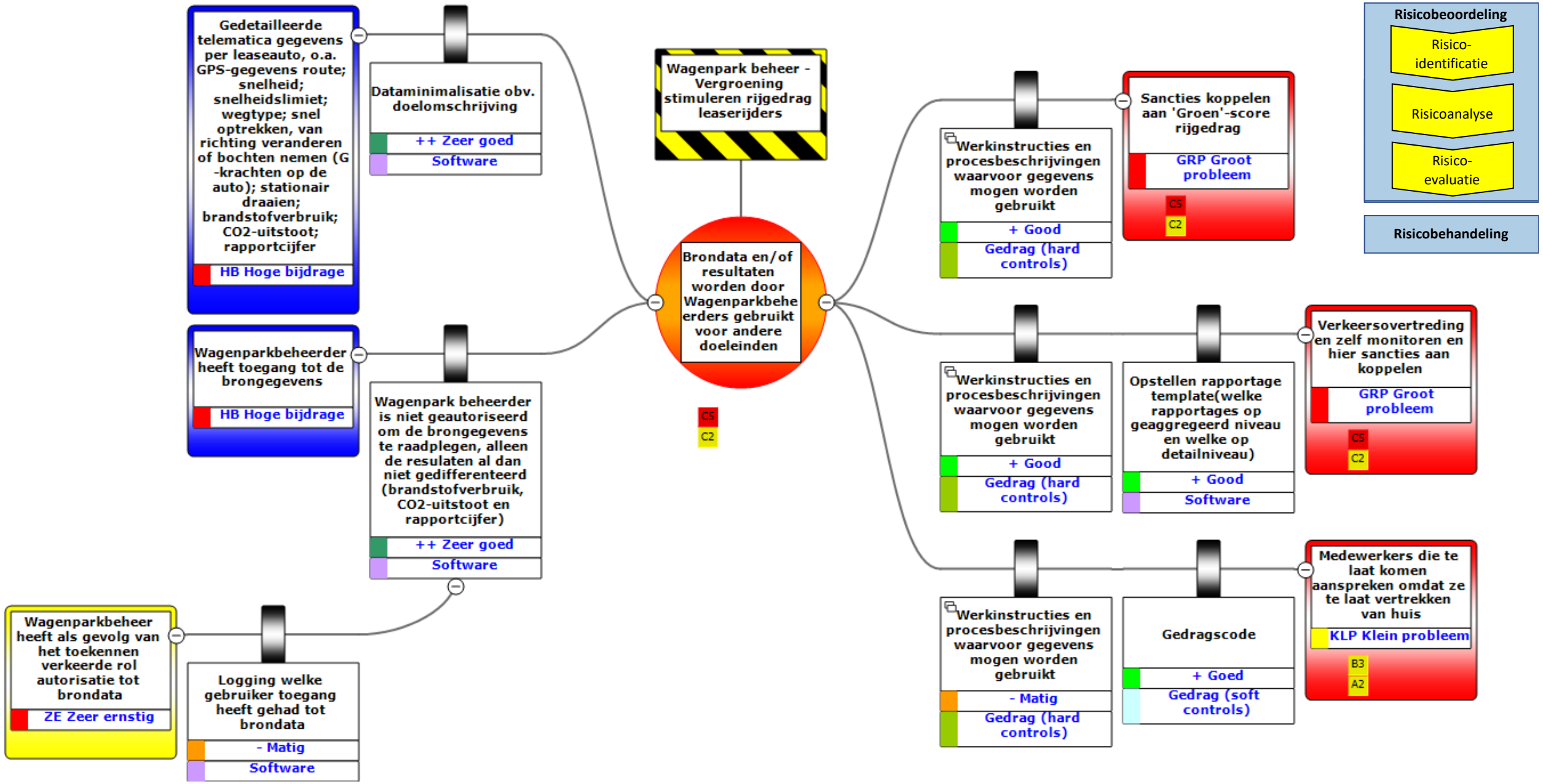
III. Risicobeoordeling en -behandeling

Raamwerk DPIA

Structuur volgen informatielevenscyc uit Privacy Contr Framework



Proces conform ISO 31000; Risicobeoordeling uitgewerkt o.b.v. BowTie (ISO31010)


Risicobeoordeling
Risico-identificatie
Risicoanalyse
Risico-evaluatie
Risicobehandeling
Wagenpark beheer - Vergroening stimuleren rijgedrag leaserijders
Brondata en/of resultaten worden door Wagenparkbeheerders gebruikt voor andere doeleinden
C5
C2
Gedetailleerde telematica gegevens per leaseauto, o.a. GPS-gegevens route; snelheid; snelheidslimiet; wegtype; snel optrekken, van richting veranderen of bochten nemen (G-krachten op de auto); stationair draaien; brandstofverbruik; CO2-uitstoot; rapportcijfer
HB Hoge bijdrage
Dataminimalisatie obv. doelomschrijving
++ Zeer goed
Software
Wagenparkbeheerder heeft toegang tot de brongegevens
HB Hoge bijdrage
Wagenpark beheerder is niet geautoriseerd om de brongegevens te raadplegen, alleen de resulaten al dan niet gedifferenteerd (brandstofverbruik, CO2-uitstoot en rapportcijfer)
++ Zeer goed
Software
Wagenparkbeheer heeft als gevolg van het toekennen verkeerde rol autorisatie tot brondata
ZE Zeer ernstig
Logging welke gebruiker toegang heeft gehad tot brondata
- Matig
Software
Werkinstructies en procesbeschrijvingen waarvoor gegevens mogen worden gebruikt
+ Good
Gedrag (hard controls)
Sancties koppelen aan 'Groen'-score rijgedrag
GRP Groot probleem
C5
C2
Werkinstructies en procesbeschrijvingen waarvoor gegevens mogen worden gebruikt
+ Good
Gedrag (hard controls)
Opstellen rapportage template(welke rapportages op geaggregeerd niveau en welke op detailniveau)
+ Good
Software
Verkeersovertreding en zelf monitoren en hier sancties aan koppelen
GRP Groot probleem
C5
C2
Werkinstructies en procesbeschrijvingen waarvoor gegevens mogen worden gebruikt
- Matig
Gedrag (hard controls)
Gedragscode
+ Goed
Gedrag (soft controls)
Medewerkers die te laat komen aanspreken omdat ze te laat vertrekken van huis
KLP Klein probleem
B3
A2

NOREA WEBINAR: PRIVACY PRODUCTEN – DPIA 2.0

Ter afsluiting

- Engelstalige versie DPIA 2.0 (naar verwachting juli 2021)
- Handreiking en Raamwerk zijn beschikbaar op website NOREA https://www.norea.nl/handreikingen

Privacy Audit Proof (PAP)

NOREA privacy-webinar

Drs. H.P. (Henk) Hendriks RE CISA
H.M. (Maurice) Koetsier MSc RE FIP CIPP/e CIPM
17 juni 2021

Inhoudsopgave

1. Inleiding
2. Privacy-auditing -
    a. Inleiding
    b. Op basis van Richtlijn 3000
    c. Op basis van SOC2/3
3. Privacy Audit Proof –
    a. Wat is het?
    b. Voorwaarden
    c. Overig
4. Beschikbare ondersteuning
5. Voorbeelden van toepassing
6. Vragen

1. Inleiding

- Per januari 2021 heeft NOREA Privacy Audit Proof opnieuw gelanceerd.
- De achtergrond van deze nieuwe lancering is de Algemene Verordening Gegevensbescherming (AVG).
- Privacy Audit Proof is een door de NOREA gedeponeerd handelsmerk.
- Doelstelling van deze presentatie is privacy auditing en het gebruik van het Privacy Audit Proof logo te promoten.
- Met Privacy Audit Proof kunnen bedrijven en instellingen aantonen dat zij een privacy audit op basis van het PCF goed hebben doorlopen.

2. Privacy Auditing

A. Inleiding

- Onderzoek naar privacy-beheersing, afgeleid uit de AVG/GDPR
- Conform Richtlijn 3000 of op basis van handreiking voor SOC 2/3
- Scope: één of meerdere verwerkingen of een deel van een verwerking
- O.b.v. PCF of andere privacy control frameworks

2. Privacy Auditing – PAP

B. Privacy-auditing op basis van Richtlijn 3000

- Richtlijn 3000 is ontleend aan de Standaard 3000 van NBA
- Belangrijkste vereisten:
  - Beschrijving object: O/B of O/B/W van de privacy-beheersing van een of meerdere (deel)verwerking van verwerkingsverantwoordelijke of verwerker
  - Normenkader: afgeleid uit AVG/ GDPR
  - Ondertekening door RE
- Dient alle relevante controledoelstellingen te omvatten evt gecombineerd met sectorale wetgeving.

Zie ook NOREA Richtlijn 3000 (Assurance-opdrachten door IT-auditors)

2. Privacy Auditing - PAP

C. Privacy-auditing op basis SOC 2/3

- Service Organization Control 2 report
  - Gebaseerd op ISAE3000
  - Rapportage volgens vaste set van criteria (beheersingsdoelstellingen). Voor Privacy gebaseerd op *GAPP Framework*
  - “Each service provider can choose its own control activities to meet the criteria, however control matrix mappings with common control frameworks are available” → biedt mogelijkheid voor invulling met PCF.

- NOREA PCF vs. SOC2 Privacy Criteria
  - FG/DPO, PIAs, Privacy by design & by default

Zie ook: NOREA Handreiking voor SOC 2 en SOC 3 o.b.v. ISAE3000 / Richtlijn 3000A

3. Privacy Audit Proof –
A. Wat is het?

- In de markt bestaat een expliciete behoefte om zichtbaar te maken dat maatregelen voor het borgen van privacy zijn genomen.
- Binnen NOREA is hiertoe het logo Privacy Audit Proof ontwikkeld.
- NOREA zorgt voor de randvoorwaarden en regelgeving met betrekking tot assurance-opdrachten.

→NOREA controleert of verifieert niet onafhankelijk de naleving van de richtlijnen

→de vertoning van het logo geeft niet 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.

Zie verder: Gebruiksvoorwaarden logo Privacy Audit Proof

3. Privacy Audit Proof –
B. Voorwaarden

Belangrijkste voorwaarden voor het toekennen/ verkrijgen:

- Assurance-rapportage met een positief oordeel zonder beperkingen
- Toepassing assurance-richtlijn Richtlijn 3000A of Handreiking voor SOC2 en SOC3
- In het eerste jaar is toets opzet/ bestaan voldoende in geval van toepassing Richtlijn 3000A
- Toepassing PCF of vergelijkbaar
- Het rapport dient te zijn voorzien van een Ondertekende management verklaring
- De long form rapportages omvat een omschrijving van het beheersingsraamwerk, inclusief testresultaten (in geval van toepassing Richtlijn 3000) of een systeembeschrijving (in geval van SOC2/3)

3. Privacy Audit Proof –
C. Overig

In de Gebruiksvoorwaarden logo Privacy Audit Proof zijn verder uitgewerkt:

- Het proces voor het aanvragen van het logo
- Gebruiksvoorwaarden voor het logo
- Tijdelijke intrekking en definitieve beëindiging van het logo
- Kwaliteitsborging en afhandeling klachten

4. Beschikbare ondersteuning

Op www.privacy-audit-proof.nl is de volgende informatie te vinden:

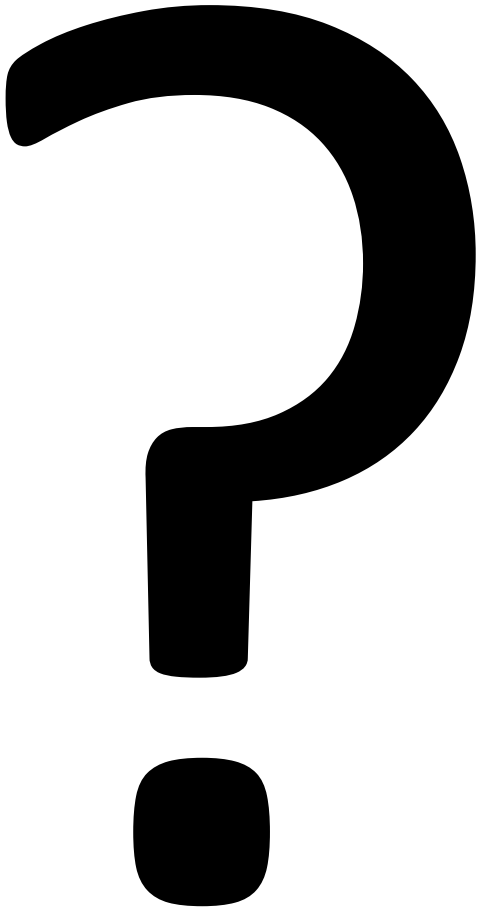
- Gebruiksvoorwaarden logo Privacy Audit Proof
- Template long-form assurance-rapport privacy
- Template short-form assurance-rapport privacy
- Template SOC3-rapport Privacy
- NOREA Handreiking Privacy Control Framework (PCF)
- Handreiking System and Organization Controls 2/3-rapporten
- Aanvraagformulier gebruik Privacy Audit Proof-logo

5. Voorbeelden van toepassing

Privacy audit Proof is van nut gebleken bij:

- Het aantonen van privacy-beheersing van bijvoorbeeld ZBO's en basisregistraties.
- Voor organisaties die grote hoeveelheden (gevoelige) persoonsgegevens verwerken als service provider
- In communicatie met toezichthoudende organen, zoals RvC's en RvT.
- Als signaal naar betrokkenen en ketenpartners.
- Voor het herwinnen van vertrouwen naar aanleiding van een incident.

6. Vragen



Bedankt voor uw aandacht!

Maurice Koetsier
BDO IT Risk Assurance
T: +31 6 53744925
M: maurice.koetsier@bdo.nl

Henk Hendriks RE CISA
hendrikshenk197@gmail.com
Tel. 06-53401880