Handboek AVG-norm Stichting AVG Garant

Versie: 8 december 2020

Dit handboek dient ter informatie voor organisaties die zich willen laten onderzoek op naleving van de AVG-norm, en voor certificeringsinstellingen[1] die geaccrediteerd zijn én een overeenkomst zijn aangegaan met de Stichting AVG Garant om onderzoeken te mogen uitvoeren op basis van deze norm. De meest actuele versie van dit Handboek is te vinden op www.avggarant.nl.

[1] In dit document wordt verder de officiële terminologie aangehouden en wordt gesproken van een conformiteitsbeoordelende instellingen (CBI).

Inhoud

1. Inleiding

Met ingang van 25 mei 2018 is de Algemene Verordening Gegevensbescherming van toepassing. Deze Europese Verordening bouwt voort op de Europese Richtlijn inzake bescherming persoonsgegevens en de daarop gebaseerde nationale privacywetgeving.

Onder deze Verordening hebben organisaties die persoonsgegevens verwerken (verwerkingsverantwoordelijken) meer verplichtingen zoals het bijhouden van een register van verwerkingsactiviteiten, aangescherpte eisen aan de grondslag 'toestemming', het uitvoeren van Data Protection Impact Assesments (DPIA's) voor hoog risico verwerkingen, het toepassen van Privacy by Design and by Default en het in sommige gevallen verplicht aanstellen van een Functionaris Persoonsgegevens. Ook hebbende personen over wie gegevens worden verwerkt ('betrokkenen) meer rechten zoals ruimere toepassing van gegevenswissing ("recht op vergetelheid"), het recht op beperking van de verwerking en het overdragen van persoonsgegevens. Ook is onder de AVG het toezicht op de naleving versterkt onder andere door de mogelijkheid van de Autoriteit Persoonsgegevens om hoge ("doeltreffende en afschrikkende") boetes op te kunnen leggen. Tenslotte is zeer kenmerkend voor de AVG dat organisaties de naleving van de AVG moeten kunnen aantonen. Ze dienen niet alleen maatregelen te nemen om conform de AVG te handelen, maar ook om dit te kunnen aantonen. Hierbij – aldus artikel 24 AVG – kunnen /organisaties zich aansluiten bij goedgekeurde gedragscodes of certificeringsmechanismen.

De Stichting AVG Garant is opgericht met als statutair doel te komen tot een certificeringsmechanisme. Haar ambitie is *om organisaties te helpen bij de uitvoering en bij het uitdragen van hun integere bedrijfsbeleid met betrekking tot persoonsgegevens*. Dit wil ze doen door organisaties te informeren, door te fungeren als spreekbuis, door het onderhouden van een norm waarmee een certificaat kan worden behaald en door het bijhouden van een register van organisaties met een behaald certificaat. Doel van dit certificaat is de naleving van de AVG te toetsen.

De Stichting heeft een norm opgesteld waarmee organisaties hun AVG-verplichtingen en "AVG-boekhouding" kunnen organiseren met het doel de AVG na te leven en deze naleving aan te tonen door middel van certificering.

Deze norm is in principe breed toepasbaar en bruikbaar voor alle organisaties, maar de focus heeft bij de uitwerking primair gelegen op de sectoren arbeidsbemiddeling en facilitaire dienstverlening. De toelichting bij deze norm is dan ook op deze sectoren gericht. Bij de ontwikkeling van de norm heeft de Stichting meerdere malen overleg gehad met betrokken brancheorganisaties.

Op verschillende niveaus vinden initiatieven plaats om te komen tot certificeringmechanismen. Door de brede scope van deze initiatieven zullen deze lastig toepasbaar zijn voor het MKB. In onze uitwerking hebben we getracht een praktische insteek te combineren met een effectieve.

Ons doel is om deze norm (formeel een conformiteitsbeoordelingsschema) op grond van artikel 42 AVG goedgekeurd te krijgen door de Raad voor Accreditatie (en de Autoriteit Persoonsgegevens). Tot het moment van goedkeuring kan nog geen AVG-certificaat verstrekt worden. Organisaties die de norm aantoonbaar naleven worden dan wel ingeschreven in het keurmerkregister van de stichting.

Dit document is opgesteld om de norm kenbaar te maken aan organisaties die zich willen laten certificeren. Ook is dit document bestemd voor Certificerende Instellingen om de norm op juiste en uniforme wijze uit te kunnen voeren. De Stichting sluit overeenkomsten met Certificerende Instellingen om te mogen toetsen op de norm.

Wijzigingen op de norm worden maximaal twee keer per jaar doorgevoerd. Input hiervoor kan zijn: ervaring van auditors, ontwikkelingen in de markt, wijziging in wet- en regelgeving (of inzichten daarin), behoeftes van het bedrijfsleven of opinies van de toezichthouder. Wijzigingen worden voorgelegd aan de klankbord van brancheorganisaties en/of de raad van advies.

In het kader van transparantie is deze norm voor iedereen in te zien. Via de website kan de norm aangevraagd worden.

Voor vragen over dit document of de norm kunt u altijd contact met ons opnemen. Dit kan via info@avggarant.nl. Voor meer informatie kunt u ook kijken op www.avggarant.nl.

Het bestuur van de Stichting AVG Garant

Theo van Leeuwen
Jeroen van Puijenbroek
Mark van Bussel

2. Wat is er geregeld over certificering in de AVG?

In artikel 42 AVG zijn de belangrijkste bepalingen over certificering opgenomen. Zo regelt lid 1 Dat de Europeesche Unie (commissie, lidstaten en toezichthouders) certificering bevordert, lid 3 dat certificering vrijwillig is en artikel 5 dat certificaten moeten worden uitgereikt door certificerende organen of door toezichthouders. In Nederland worden certificaten uitgereikt door certificerende organen. is het eerste geregeld. Het gaat hierbij om conformiteitsbeoordelende instellingen (CBI's of certificerende instellingen) die hiervoor door de Raad van Accreditatie zijn geaccrediteerd.

Wil een CBI geaccrediteerd kunnen worden dan dient deze de norm EN-ISO/IEC 17065[2], de eisen uit het certificatieschema (de AVG-norm) en de aanvullende eisen van de AP te kunnen toepassen. Na accreditatie dient een CBI periodiek gecontroleerd te worden.

Het certificatieschema kan ook door derden opgesteld en beheerd worden, zoals bij de Stichting AVG Garant aan de orde is.

Bij een verzoek tot accreditatie van het schema (de norm) zal de RvA een vooronderzoek doen en bij een positieve afronding de Autoriteit Persoonsgegevens (AP) verzoeken een oordeel te geven over het te gebruiken schema. De AP stemt hierbij haar standpunt af met de European Data Protection Board (het samenwerkingsverband van Europese toezichthouders/EDPB).

Om een schema te kunnen beheren moet de beheerder onder andere aantonen dat er voor het schema draagvlak is in de markt en dat deze overeenkomsten heeft gesloten met geaccrediteerde CBI's om audits op basis van deze norm uit te voeren. Verder moet de schemabeheerder aantonen dat hij over de juiste competenties beschikt om het schema op te stellen en te onderhouden. Tenslotte moet hij een eigen validatie hebben uitgevoerd. Hierin toont hij aan – zowel in theorie als in praktijk – dat het doel van het schema ook wordt bereikt met de beoordelingen.

De Stichting AVG Garant heeft op dit moment een overeenkomst met Bureau Cicero om in gezamenlijkheid een accreditatie aan te vragen.

Wel heeft de EDPB een richtlijn opgesteld. Hierin worden een aantal elementen aangehaald die aan de orde moeten komen in het schema bijv. de rechtmatigheid, de principes van verwerking, de meldplicht datalekken etc.. Ook valt in de richtlijnen te lezen dat criteria uniform, verifieerbaar en auditbaar moeten zijn. Daarnaast moet de norm schaalbaar zijn en toepasbaar in andere branches.

3. Voordelen AVG Certificering

De AVG noemt een aantal voordelen van certificering. Met een AVG-certificaat kun je naleving aantonen (zie bijvoorbeeld de artikelen 24 – 3 (naleving), artikel 28 – 5 (bewijs bij verwerkers dat ze AVG naleven) en artikel 32 – 3 (bewijs dat aan beveiligingseisen wordt voldaan). Daarnaast is in de boete-artikelen van de AVG geregeld dat bij het vaststellen van de boetes rekening wordt gehouden met het al of niet gecertificeerd zijn. Maar de wet geeft ook aan: een certificaat ontslaat de verwerkingsverantwoordelijke en de toezichthouder verder niet van hun verplichtingen.

In commercieel opzicht kan een certificering aantrekkelijk zijn. Denk aan het voldoen aan tendereisen of het anderszins vergroten van het onderscheidend vermogen, niet alleen richting klanten maar ook richting andere betrokkenen zoals medewerkers

Verder kan het u helpen bij het kiezen van verwerkers. Als u een verwerker inschakelt blijft u verantwoordelijk voor de naleving van de AVG. Met een certificaat is dit makkelijker aan te tonen.

[2] Certificatie volgens ISO/IEC 17065 heeft tot doel dat vertrouwen gecreëerd wordt dat een product, proces of dienst voldoet aan alle gespecifieerde vereisten zowel initieel als tijdens de levensduur van het product. De norm bepaalt de vereisten waaraan een certificatie-instelling moet voldoen om derde-partij certificatie aan te bieden op een competente, consistente en onafhankelijke manier.

Ook kan een certificering organisaties helpen bij het verbeteren en up-to-date houden van de processen en verwerking van uw persoonsgegevens.

4. Stappen naar certificatie en registratie

Om in aanmerking te komen voor een onderzoek dat leidt tot certificering en registratie dienen de volgende stappen ondernomen te worden.

1. De organisatie meldt zich aan bij de Stichting AVG Garant en gaat een registratie-overeenkomst aan op grond waarvan, naast eenmalige inschrijfkosten, een jaarlijkse fee dient te worden betaald.
2. De organisatie gaat een certificatieovereenkomst aan met een CBI die een overeenkomst heeft met de Stichting.
3. De organisatie verstrekt relevante informatie over de organisatie en zijn activiteiten en levert de gevraagde (privacy) documenten aan bij de CBI.
4. De CBI voert het certificatieonderzoek uit - waarbij per normpunt naleving wordt nagegaan - en legt het resultaat hiervan vast.
5. De CBI verstrekt bij een positief resultaat een certificaat.
6. De CBI informeert de organisatie en de stichting.
7. De Stichting besluit tot registratie en legt - indien de organisatie aan zijn overige verplichtingen uit het registratiereglement heeft voldaan – de certificering vast in het openbare[3]register.
8. De CBI maakt afspraken met de organisatie over het onderhoud en vervolgonderzoeken.

Een onderzoek bestaat uit de volgende stappen:

1 Bestudering aangeleverde documenten.
2 Gesprek met stakeholders[4]binnen organisatie.
3 Eventueel een gesprek op vestigingen.
4 Bekijken van belangrijkste persoonsgegevens verwerkende systemen (‘walk through’).
5 Steekproefsgewijze controle en inspecties: bijv. van documenten, procedures en/of dossiers.
6 Indien noodzakelijk: controle van een of meerdere vestigingen.
7 Opstellen rapport door onderzoekers en bespreken met directie.
8 Al of niet verstrekken van certificaat.
9 Maken van vervolgafspraken.

In het onderzoek worden opzet, bestaan en werking van de in scope zijnde verwerkingen en het privacymanagementsysteem getoetst langs de lijnen van de verschillende normpunten (zie verder hoofdstuk 7).

Volgens de AVG is een certificaat maximaal drie jaar geldig. De Stichting AVG Garant heeft deze periode overgenomen. Iedere drie jaar vindt er dan ook een integrale toetsing plaats op naleving van de normpunten.

Wel moeten gecertificeerde organisaties blijvend aantonen dat ze aan de normen voldoen. Vandaar dat er jaarlijkse een “onderhoudscontrole” plaatsvindt. In deze onderhoudscontroles zal de focus vooral liggen op wijzigingen en gebeurtenissen in het achterliggende jaar die voor de naleving van de AVG van belang zijn én de werking van beleid en procedures (zie verder hieronder). Overigens moeten gecertificeerde organisaties wijzigingen die van belang zijn voor de certificering en de naleving van de AVG[5] aan hun CBI doorgeven, en deze conform wet en norm gedocumenteerd doorvoeren.

In de onderhoudsonderzoeken zal door de CBI aandacht besteed worden aan:

- Beleids- en organisatiewijzigingen met impact op naleving van de AVG (denk aan overnames, nieuwe producten etc.);

[3] www.avggarant.nl
[4] Gesprek met minimaal: de hoogst (directie) verantwoordelijke voor bescherming persoonsgegevens, de voor de uitvoering van het privacybeleid verantwoordelijke, en de voor de technische maatregelen verantwoordelijke (IT-) manager.
[5] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - Annex 1

- Nieuwe (of sterk gewijzigde) verwerkingen (controle op register, DPIA, privacystatement, verwerkersovereenkomst etc.);
- Nieuwe of gewijzigde procedures;
- Wijzigingen in privacybeleid en/of rolverdeling;
- Rapportages incidenten/datalekken en verzoeken betrokkenen;
- Eventuele verzoeken of onderzoeken van de Autoriteit Persoonsgegevens;
- Verrichtte inspanningen. om kennis en bewustzijn medewerkers te vergroten;
- Wijzigingen in informatiebeveiligingsbeleid en IT-infrastructuur;
- Eventueel onderzoek van verwerkingen die tijdens vorige onderzoek minder aan bod zijn gekomen;
- Update actiepunten (bijvoorbeeld naar aanleiding van een eerder certificeringsonderzoek of een interne audit).

5. Scope van de certificering

De certificering heeft betrekking op verwerking van persoonsgegevens die plaatsvinden binnen de aangemelde organisatie (rechtspersoon) of de aangemelde organisaties. De certificering richt zich uitsluitend op Nederlandse organisaties die verwerkingsverantwoordelijke zijn en die bedrijfsmatig werkzaamheden verrichten in de sector arbeidsbemiddeling (SBI 780), facilitaire dienstverlening (SBI 810), overige zakelijke dienstverlening (SBI 820) en dienstverlening voor de landbouw (SBI 160). AVG Garant beperkt zich hierbij tot de gegevensverwerkingen in Nederland.

De tekst van het certificaat is als volgt:

CBI> verklaart dat het proces van de verwerking van persoonsgegevens van <naam onderneming> met <kvk-nummer> te <plaats> voldoet aan de eisen van het certificatieschema:

AVG Garant, versie xxxx.

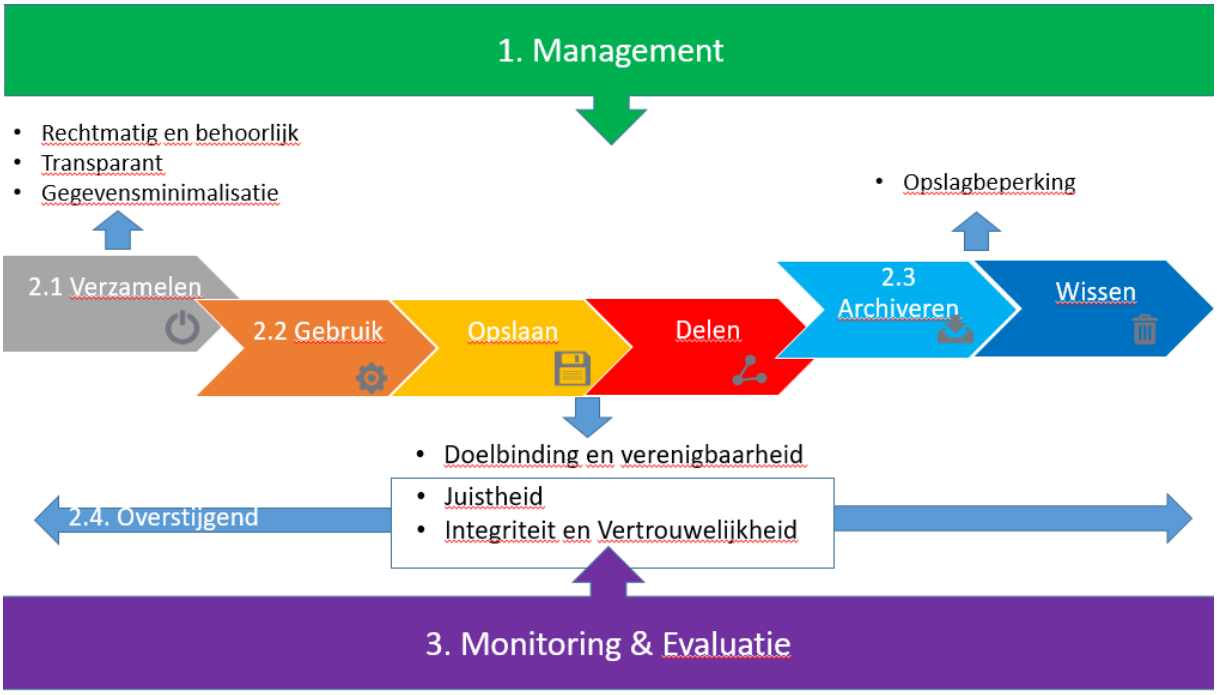
6. Samenwerking & kwaliteit Certificerende Instellingen (CBI's)

CBI's die audits onder de AVG Garant norm willen uitvoeren dienen daartoe een overeenkomst te hebben gesloten met de stichting. In deze certificatieovereenkomst worden vooral afspraken vastgelegd ten aanzien van kwaliteit en werk- en rapportageprocedures. Van belang is dat een CBI geaccrediteerd is om audits (zie voor aanvullende eisen ook de guideline genoemd in voetnoot 4) te doen en aantoont dat ze het normschema onverkort toepast.

Periodiek wordt de AVG Garant norm geëvalueerd door het College van Deskundigen. Dit College adviseert het bestuur gevraagd en ongevraagd over aanpassingen van de norm op basis van de ervaring en achtergrond van de leden van het College. De leden baseren zich op wijzigingen in wet- en regelgeving, relevante jurisprudentie, praktijkervaring et cetera. Voor het College van Deskundigen is een apart reglement opgesteld. Knelpunten en interpretatievraagstukken worden met de CBI's besproken in het harmonisatieoverleg.
Aan het auditerende personeel worden in het certificatiereglement eisen ten aanzien van kennis en ervaring gesteld. Op initiatief van de stichting is de AVG Garant Audit-training in de markt beschikbaar gekomen.
Op grond van de accreditatie eisen dient de CBI ook een klachtenregeling geïmplementeerd te hebben. Tenslotte is er in het reglement de mogelijkheid opgenomen om op verzoek van het bestuur CBI's extern te laten auditen.

7. Aanpak norm

Bij het opstellen van de norm is de stichting niet uitgegaan van de volgorde die de wet hanteert, maar heeft ze ervoor gekozen om deze op te zetten langs de processtappen van de verwerking van persoonsgegevens. Hierbij wordt aansluiting gezocht bij de cyclische managementaanpak van organisaties bij het realiseren van de organisatiedoelen. De cyclus bestaat hierbij uit het vaststellen van beleid en het organiseren van processen, de processen zelf en een evaluatie en bijsturing (de zogenaamde PDCA-cyclus). Hiermee wordt beoogd de bescherming van persoonsgegevens onderdeel te laten maken van de managementcyclus[6]. In figuur 1 is dit grafisch weergegeven



figuur 1

In stap 1 worden de activiteiten beschreven die door het management dienen te worden uitgevoerd en/of generiek van aard zijn. Denk aan het opstellen van privacybeleid, rollen en verantwoordelijkheden, training en awareness, of omgaan met rechten van betrokkenen of het onderhouden van een verwerkingenregister. In stap 2 worden de activiteiten van de verwerking omschreven vanaf het verzamelen van persoonsgegevens tot en met het verwijderen daarvan plus de overschrijdende eisen zoals het juist en integer houden van de persoonsgegevens. In stap 3 is vervolgens de monitoring en evaluatie opgenomen.

Op de drie stappen zijn - conform het onderstaande schema - de normpunten van toepassing die in hoofdstuk 11 zijn uitgeschreven.

[6] De Stichting hanteert hierbij een vergelijkbare aanpak als Norea (Privacy Control Framework).

I. MANAGEMENT	II. LEVENSCYCLUS	III. MONITORING EN EVALUATIE
	II.1. VERZAMELEN	
1. Privacybeleid	12. Rechtmatige verwerking	22. Monitoring en evaluatie
2. Rollen & Verantwoordelijkheden	13. Toestemming	
3. Verwerkingenregister	14. Informatie betrokkenen	
4. Verwerking buiten de EU	15. Dataminimalisatie	
5. Data Protection Impact Assessment	**II.2. OPSLAAN, GEBRUIK, DELEN**	
6. Verwerkersovereenkomsten	16. Doelbinding	
7. Incident- en datalekregistratie	17. Verstrekking aan derden	
8. Kennis & competentie medewerkers	**II.3. ARCHIVEREN EN WISSEN**	
9. Monitoren privacy ontwikkeling	18. Bewaartermijnen	
10. Uitvoeren rechten betrokkenen	**II.4. OVERSTIJGEND**	
11. Privacy by design & by default	19. Passende beveiligingsmaatregelen	
	20. Toegangsrechten en Authenticatie	
	21. Juist houden gegevens	

8. Beoordeling

Bij het onderzoek zal de auditor per normpunt vaststellen of de waargenomen situatie aan de norm voldoet[7]. Bij tekortkomingen geeft hij de mate van de tekortkoming in overeenstemming met onderstaand schema aan. De Stichting heeft in de "Handreiking beoordeling norm Stichting AVG Garant" richtlijnen opgenomen voor de beoordeling. Afhankelijk van de concrete aangetroffen situatie kan een auditor altijd beslissen tot een op- of afwaardering van de ernst van de afwijking.

Conformiteitscore

	Niet-materiële tekortkoming (Significantie norm: Laag)	Materiële tekortkoming (Significantie norm: Hoog)
Structurele tekortkoming	Deficiëntie	Non-conformiteit
Incidentele tekortkoming	Incident	Deficiëntie

Per normpunt is in de norm de significantie (Hoog/Laag) aangegeven. Hierbij is rekening gehouden met het belang dat de Autoriteit Persoonsgegevens aan de verschillende wettelijke verplichtingen heeft toegekend door middel van de boetebeleidsregels 2019 èn het belang van het hebben van een privacymanagementsysteem waarmee op structurele basis richting gegeven kan worden aan het de AVG en het privacybeleid.

Het niet voldoen aan een norm met een hoge significantie is een materiële tekortkoming; het niet voldoen aan een norm met een lage significatie leidt tot een niet-materiële tekortkoming. Een tekortkoming kan incidenteel of structureel zijn. Het is de bevoegdheid van de auditor om dit vast te stellen.

Van een tekortkoming van de naleving van de norm is sprake wanneer er een nadelig effect op de privacybescherming van betrokkenen optreedt. De Stichting heeft in de "Handreiking beoordeling norm Stichting AVG Garant" voorbeelden van incidentele en structurele tekortkomingen.

Bij een non-conformiteit wordt geen certificaat verstrekt of wordt deze ingetrokken, tenzij deze binnen 30 dagen aantoonbaar gecorrigeerd is. Indien noodzakelijk vindt er bij deze correctie aanvullend onderzoek plaats. Voor de overige afwijkingen geldt voor het te nemen besluit ten aanzien van het verstrekken of intrekken van een certificaat onderstaande tabel.

Geconstateerde tekortkomingen	**Nieuw certificaat**	**Bestaand certificaat (herhaling audit)**
1 of meer non-conformiteiten	Niet verstrekken	Intrekken, tenzij binnen 30 dagen aantoonbaar hersteld is. Max. 1 non-conformiteit; anders direct opschorten.
meer dan 2 deficiënties	Niet verstrekken	Intrekken, tenzij binnen 60 dagen aantoonbaar hersteld is. Max 4 deficiënties; anders direct opschorten.
meer dan 5 incidenten	Niet verstrekken	Intrekken, tenzij deze binnen 90 dagen aantoonbaar hersteld is. Max. 8 incidenten; anders direct opschorten.
2 deficiënties en meer dan 1 incident	Niet verstrekken	Intrekken, tenzij deficiënties binnen 60 dagen aantoonbaar

[7] De Stichting AVG Garant heeft voor CBI's een Handreiking opgesteld die dient als hulpmiddel om conformiteit vast te stellen.

		zijn hersteld en incidenten binnen 90 dagen.
1 deficiëntie en meer dan 3 incidenten	Niet verstrekken	Intrekken, tenzij deficiëntie binnen 60 dagen aantoonbaar zijn hersteld en incidenten binnen 90 dagen.
1 deficiëntie en minder dan of gelijk aan 3 incidenten	Niet verstrekken	Behouden (onder voorwaarde dat deficiënties binnen 60 dagen, en incidenten binnen 90 dagen aantoonbaar worden hersteld).

9. Integrale of steekproefsgewijze controle

Bij het onderzoek worden de normpunten integraal of steekproefsgewijs gecontroleerd. Zo worden bijvoorbeeld privacybeleid en verwerkingsregister integraal beoordeeld. Steekproefsgewijze controle vindt bijvoorbeeld plaats op verwerkingen, verwerkersovereenkomsten en maatregelen. Bij de selectie wordt onder andere rekening gehouden of het een hoog risico verwerking betreft of een verwerking waar toestemming de grondslag is. De Stichting heeft in de “Handreiking beoordeling norm Stichting Garant” deze aanpak nader uitgewerkt.

10. Gehanteerde definities

Voor wat betreft de definities sluiten we aan bij de definities uit de AVG (art. 4) en de UAVG art. 1. Voor wat betreft certificering onder de AVG sluiten we aan bij de definities van de European Data Protection Board. Tenslotte sluiten we voor operationele termen aan bij wat gebruikelijk is (o.a. ISO 27001/9001). Zie verder bijlage 2.

11. Normpunten

1. MANAGEMENT

1. Privacybeleid

Beschrijving normpunt:

De organisatie heeft een gedocumenteerd (privacy)beleid welk bekend is gemaakt bij de medewerkers.

Significantie[8] *normpunt:*
Hoog

AVG[9]:
Artt. 5.2, 24.2, 39

Onderbouwing:

Op grond van artikel 24 moet een organisatie een privacybeleid hebben waarmee zij de naleving kan borgen en aantonen. Dit beleid dient bekend te zijn bij de medewerkers. Het beleid dient als startpunt voor de audit en wordt door de certificerende instelling meegenomen in het gesprek met de organisatie. Tijdens de audit wordt er gecontroleerd op consistentie en compliance: worden genoemde ambities en doelstellingen verder in de audit teruggezien.

Toelichting:
Het privacybeleid is verplicht voor zover dit 'in verhouding staat tot de verwerkingsactiviteiten'. Dit is altijd het geval als er bijzondere gegevens of BSN worden verwerkt.

De AVG stelt geen eisen aan inhoud of vorm van dit beleid. Wel heeft de AP een aanbeveling gedaan. In het kort komt die erop neer dat een beleid niet versnipperd moet zijn en toegeschreven moet zijn naar de situatie van de organisatie. Wat de AP betreft bevat dit beleid ten minimale de soort gegevens die verwerkt worden, de doeleinden waarvoor en de rechten van betrokkenen.

Het ligt voor de hand om in een privacybeleid ook de overige onderwerpen uit de AVG én deze norm terug te laten komen. Mogelijke onderwerpen zijn dan:

- Visie op omgang met persoonsgegevens
- Taken en verantwoordelijkheden (inrichting "privacy governance", wel/niet FG);
- De rollen die de organisatie vervult (verwerkingsverantwoordelijke/verwerker)
- De invulling van privacybeginselen (denk aan bewaarbeleid of dataminimalisatie);
- De soort gegevens en op hoofdlijnen de doeleinden waarvoor deze worden verwerkt;
- Beheer verwerkingenregister en overzicht met wie gegevens gedeeld worden;
- Omgang met (nieuwe) verwerkingen (DPIA procedures, Privacy by Design and Default);
- Wijze van communicatie naar betrokkenen ("privacystatement");
- Omgang met risico's en informatiebeveiligingsbeleid;
- Omgang met incidenten en datalekken;

[8] Elk normpunt heeft zijn significantie (hoog of laag); zie paragraaf 8.
[9] Verwijzing naar relevante artikelen uit de AVG en/of de UAVG.

- Omgang met de rechten van betrokkenen;
- Omgang van Awareness en kennis bij medewerkers;
- Monitoring en evaluatie (plan-do-check-act).

Het format is vormvrij en kan zijn: beleidsplan, privacyplan, missie en gedragsregels, instructies etc..
Bekendmaking aan medewerkers kan plaatsvinden via mail, post of intranet etc..

Branche-kleuring:
Te denken valt aan afspraken over de omgang van bijzondere persoonsgegevens waaronder ook BSN en strafrechtelijke gegevens (VOG), het wel of niet aanstellen van een FG, de opleiding van medewerkers, het beleid t.a.v. profilering, genomen maatregelen, het delen van gegevens met derden waaronder opdrachtgevers, etc..

Hulpmiddelen:
- https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/zes-aanbevelingen-voor-een-privacybeleid
- Zie blog AVG Garant op Flexnieuws: https://avggarant.nl/geen-categorie/is-hebben-van-een-privacybeleid-verplicht

2. Rollen & Verantwoordelijkheden

Beschrijving normpunt:

2.1. De organisatie weet welke rol zij vervult bij de verschillende verwerkingen: als verwerkingsverantwoordelijke, als verwerker of als gezamenlijk verantwoordelijke, en heeft dit gedocumenteerd.

Significantie normpunt:
Hoog

AVG:
Artt. 24.2, 28.1, 30.1a,d, 30.2.

Onderbouwing:
Om de verplichtingen uit de AVG na te komen is het van belang dat het helder is welke rol de organisatie vervult bij de verschillende verwerkingen. Doorgaans worden de verschillende rollen vanuit de aard van de dienstverlening beschreven in het privacybeleid.
Daarnaast kunnen de rollen opgenomen zijn in de verwerkingenregisters of in enige ander document.

Toelichting:
Als de organisatie een verwerkingsverantwoordelijke is dient zij de verwerkingen op te nemen in een verwerkingenregister en hierin aan te geven met welke derde partijen de gegevens gedeeld worden. Het ligt hierbij voor de hand dat hierin dan ook opgenomen wordt of die derden verwerkers zijn. Is dit niet het geval dan kan dit ook in enige ander document opgenomen zijn. In dit verwerkingsregister moet de organisatie ook de namen van eventueel gezamenlijke verwerkingsverantwoordelijken opnemen.

Als de organisatie (als verwerker) ten behoeve van andere verwerkingsverantwoordelijke persoonsgegevens verwerkt moet zij deze verwerkingen vastleggen in een apart register.
Uit dit register blijkt dus de rol van verwerker.

Branche-kleuring:
Uitzendbureaus en ZZP-bemiddelaars zijn in de meeste gevallen bij de uitvoering van hun dienstverlening verwerkingsverantwoordelijke. Daar waar ze verwerker zijn moet het helder zijn dat er persoonsgegevens in opdracht van derden worden verwerkt zonder dat ze dit doen in het kader van

hun eigen dienstverlening. Zie verder normpunt 6.3. Gezamenlijke verantwoordelijkheid komt o.a. voor daar waar intermediairs en backoffice payroll organisaties gezamenlijk optreden.

Hulpmiddelen[10]?:
Handleiding AVG (min J&V), met name schema 3.
EDPB Opinion 1/2010 on the concepts of "controller" and "processor"
https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/02/Factsheet-en-Beslismodel-Verwerker-Verwerkingsverantwoordelijke-v1.1.pdf
www.wecglobal.org, Industry guidelines clarify rules for HR Service Providers

Beschrijving normpunt:

2.2. Binnen de organisatie is het duidelijk bij wie de verantwoordelijkheden inzake het beheer en de bescherming van persoonsgegevens zijn belegd.

Significantie normpunt:
Laag

AVG:
Artt. 24.1, 37.1

Onderbouwing:
De organisatie moet kunnen aantonen aan wie deze verantwoordelijkheden zijn toegedeeld. Dit kan bijvoorbeeld blijken uit beleid, functieprofielen of taaktoewijzingen. Grote organisaties moeten aantonen of de aanstelling van een Functionaris Gegevensbescherming verplicht is en als dat het geval is of ze deze hebben aangesteld.

Toelichting:
Bij kleine organisaties is vaak de directeur de verantwoordelijke; bij grotere organisaties zal vaak sprake zijn van functiedifferentiatie en krijg je scheiding in functies (RACI: responsible, accountable, consulted, informed).
Als er een FG is aangesteld, dient vastgesteld te worden of deze vrijwillig of verplicht is aangesteld en of benoeming of aanstelling overeenkomstig de regels van de AVG is gedaan (gemeld aan AP, onafhankelijkheid geborgd, kenbaar gemaakt aan derden, voldoen aan functie-eisen).

Branche-kleuring:
Een FG moet worden ingesteld in de situaties zoals in de wet genoemd. Dit zal niet vaak het geval zijn binnen de bemiddelingsbranche, omdat de verwerking van bijzondere persoonsgegevens niet de kerntaak van een uitzender is. Een FG kan aan de orde zijn als de organisatie erg groot is of indien er op grote schaal monitoring en/of profilering plaatsvindt.

Hulpmiddelen:
Checklist FG van de NBBU[11].
Checklist FG op https://www.ngfg.nl
De AP over grootschaligheid: https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-uitleg-over-grootschalige-gegevensverwerking-de-zorg
https://www.flexnieuws.nl/nieuws/is-een-functionaris-voor-de-gegevensbescherming-verplicht/

Beschrijving normpunt:

2.3 Er is vastgelegd wat de organisatie van haar medewerkers verwacht t.a.v. de omgang met persoonsgegevens.

[10] Op avggarant.nl is een overzicht beschikbaar van informatie over de AVG. Dit overzicht zal in de loop der tijd actueel worden gehouden en aangevuld.
[11] Om toegang te krijgen tot de documenten van de brancheorganisaties moeten ondernemingen lid zijn.

Significantie normpunt:
Laag

AVG:
Artt. 39.1b, 24.1

Onderbouwing:
De organisatie toont deze rollen en verantwoordelijkheden aan en hoe ze deze gecommuniceerd heeft. Dit kan vastgelegd zijn in privacy beleid, gedragsregels, arbeidsovereenkomsten, protocollen en/of opgenomen zijn in awareness- of trainingsprogramma's waaronder e-learning.

Toelichting:
Denk aan geheimhouding, omgang met persoonsgegevens richting klanten, het gebruik van middelen en systemen, melden incidenten en datalekken, verantwoordelijk gebruik internet en email etc..

Branche-kleuring:
-

Hulpmiddelen:
-

3. Verwerkingenregister

Beschrijving normpunt:

De organisatie onderhoudt en beheert een register van alle verwerkingen overeenkomstig de verplichtingen uit de AVG. Daar waar de organisatie als verwerker optreedt onderhoudt en beheert zij daarvoor een apart register.

Significantie normpunt:
Hoog

AVG:
Art. 30.

Onderbouwing:
De organisatie toont aan dat ze een of meerdere verwerkingenregisters heeft, en ze toont aan dat deze registers volledig en juist zijn gevuld.

Toelichting:
De AVG schrijft geen format voor. Wel worden er een aantal elementen genoemd die verplicht opgenomen moeten worden. Voor het register van verwerkingen als verwerkingsverantwoordelijke zijn dit:

- Naam en contactgegevens van de verwerkingsverantwoordelijke inclusief die van een eventuele FG;
- De doeleinden;
- De beschrijving van de categorieën van betrokkenen;
- De categorieën van ontvangers;
- De evt. doorgifte aan derde landen;
- De bewaartermijnen;
- Een algemene beschrijving van beveiligingsmaatregelen.

De verwerkingsverantwoordelijke moet kunnen aantonen dat de verwerkingen rechtmatig zijn (zie normpunt 12). Om te voorkomen dat de grondslag in een apart register wordt bijgehouden kan dit

element ook worden worden opgenomen in het verwerkingenregister. Hetzelfde geldt voor het risiconiveau van de verwerking om te bepalen of er een Data Protection Impact Assessment (DPIA) vereist is (zie normpunt 5).

Voor het register die de organisatie als verwerker opstelt zijn de volgende elementen verplicht:

- Naam en contactgegevens van de organisatie inclusief die van de verwerkingsverantwoordelijke voor ze persoonsgegevens verwerkt, en inclusief die van een eventuele FG;
- De categorieën van verwerkingen;
- De eventuele doorgifte aan derde landen (buiten de EU/EER);
- Een algemene beschrijving van beveiligingsmaatregelen

Zoals gezegd is het register vormvrij. Van belang is dat de ondernemer aantoont dat het register zowel volledig (bevat het alle verwerkingen en alle verplichte elementen), als juist (is de inhoud juist en actueel) is. Een register kan zowel gevuld worden aan de hand van processen waarlangs persoonsgegevens lopen, als aan de hand van voor persoonsgegevens gebruikte systemen of applicaties. Een register dient voldoende gedetailleerd te zijn om bruikbaar te zijn voor de naleving van de AVG.

Branche-kleuring:
Belangrijke verwerkingen die minimaal terug moeten komen zijn o.a.: recruitment (medewerkers en zzp'ers), selectie, verloning, facturering, plaatsing bij opdrachtgevers, ziekmeldingen.

Hulpmiddelen:
Format verwerkingenregister: ABU, NBBU
Format verwerkingenregister: AVG Flex Oké, wedoprivacy.com (deels al ingevuld voor uitzendbureaus)

4. Verwerking buiten de EU/EER

Beschrijving normpunt:

De organisatie weet welke verwerkingen buiten de EU/EER[12] plaatsvinden, en heeft daar waarborgende maatregelen voor getroffen.

Significantie normpunt:
Hoog

AVG:
Artt. 13.1e, 30.1e, 44-47, 49

Onderbouwing:
De organisatie toont door middel van het verwerkingenregister aan wanneer er sprake is van een doorgifte naar derde landen en welke passende waarborgen hij in dat kader heeft genomen.

Toelichting:
Uitgangspunt is dat gegevens in de EU/EER moeten worden verwerkt. Voor verwerking buiten EU/EER geldt dat er extra waarborgen geboden moeten worden om te voorkomen dat het beschermingsniveau van de AVG ondermijnd wordt. De AVG kent verschillende waarborgen waaronder de belangrijkste zijn:

[12] Europeesche Economische Ruimte (EER): Lidstaten van de EU plus Liechtenstein, Noorwegen en IJsland. Het Verenigd Koninkrijk is vanaf 31 jan. 2020 geen EU/EER-lidstaat meer maar tijdens de overgangsperiode tot en 31 dec. 2020 blijven de rechten volgens EU-regels gelden.

- Verstrekking aan derde landen waarvoor een adequaatheidsbesluit van de Europese Commissie is afgegeven;
- Gebruik van bindende bedrijfsvoorschriften:
- Gebruik van EU-modelovereenkomst;

In juli 2020 heeft het Europese Hof van Justitie het Privacyshield, een veel gebruikt waarborg om persoonsgegevens aan organisaties in de Verenigede Staten te mogen verstrekken, ongeldig verklaard omdat deze te weinig bescherming biedt. Het Hof heeft tevens bepaald dat de EU-modelovereenkomsten gebruikt kunnen worden, maar alleen als een gelijkwaardig beschermingsniveau in de praktijk kan worden gewaarborgd. De European Data Protecion Board stelt aanbevelingen op om hier vorm aan te kunnen geven.

Branche-kleuring:
Belangrijke verwerkers zijn partijen die op de branche gerichte software aanbieden voor recruitment en/of verloning. Vaak vindt de verwerking/opslag binnen de EU/EER plaats. Qua kantoorautomatisering wordt vaak gebruik gemaakt van partijen buiten de EER. Denk aan Microsoft, Mailchimp, Dropbox, etc.. Check dan waar de data worden opgeslagen. Veel Amerikaanse organisaties gaan ertoe over om data in de EU/EER op te slaan. Let op: zorg wel altijd voor een verwerkingsovereenkomst.

Hulpmiddelen:
Handleiding AVG: Min J&V, hoofdstuk 8
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
EC Standard Contractual Clauses (SCC)
Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data
Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

5. Data Protection Impact Assessment

Beschrijving normpunt:

De organisatie voert een Data Protection Impact Assessment (DPIA) uit in die situaties dat dat verplicht is.

Significantie normpunt:
Hoog

AVG:
Art. 35

Onderbouwing:
De organisatie toont met instructies of procedures aan dat er bij nieuwe verwerkingen vastgesteld wordt of er een DPIA vereist is, dat de noodzaak van een DPIA voor alle verwerkingen is vastgesteld en welke DPIA's er zijn uitgevoerd.

Toelichting:
Een DPIA is in ieder geval verplicht bij verwerkingen die een hoog privacyrisico opleveren, zoals de verwerkingen die in de AVG worden genoemd:
- bij grootschalige verwerking van bijzondere persoonsgegevens;
- bij stelstelmatige en grootschalige monitoring van openbare ruimtes,

- bij systematische en uitgebreide beoordeling op basis van automatische besluitvorming (denk aan profilering).

Ter concretisering heeft de AP een lijst samengesteld van verwerkingen waarvoor een DPIA altijd verplicht is. Daarnaast dient de organisatie zelf te bepalen of een verwerking een hoog privacyrisico oplevert en een DPIA vereist is. Als hulpmiddel heeft de Europese toezichthouder 9 criteria benoemd, waarbij de handreiking is dat indien er twee van toepassing zijn op de verwerking er een DPIA vereist is.

Branche-kleuring:
Gezien de richtlijnen van de AP en de Europese toezichthouder zal een DPIA in de uitzendbranche niet snel aan de orde zijn. Tegelijkertijd zijn een aantal criteria van de lijst van 9 in toenemende mate van toepassing in de uitzendbranche. Denk aan het gebruik van nieuwe technologieën, profilering, geautomatiseerde besluitvorming en de verwerking van gevoelige gegevens. Als belangrijk criterium geldt ook hier de grootschaligheid van verwerkingen. De kans op een verplichte DPIA neemt aanzienlijk toe boven de 10.000 verwerkte dossiers.

Hulpmiddelen:
Model DPIA (ABU)

Om vast te stellen of een DPIA vereist is:
https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia
https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667
https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#wat-zijn-de-criteria-van-de-europese-privacytoezichthouders-6668

Om DPIA uit te voeren:
https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
https://www.privacy-friendly.nl/dpia

6. Verwerkersovereenkomsten

Beschrijving normpunt:

6.1. De organisatie zorgt ervoor dat wanneer zij als verwerkingsverantwoordelijke verwerkingen uitbesteed aan een verwerker dat er vóór aanvang van die uitbesteding een overeenkomst is overeengekomen waarin minimaal de onderwerpen zijn opgenomen overeenkomstig de bepalingen in de AVG.

Significantie normpunt:
Hoog

AVG:
Art. 28

Onderbouwing:
De organisatie toont aan dat zij met alle verwerkers een verwerkersovereenkomst heeft afgesloten, en dat deze voldoen aan de eisen van de AVG

Toelichting:
In artikel 28 zijn de onderdelen opgenomen die minimaal in een verwerkersovereenkomst moeten worden opgenomen.
Volgens de handleiding AVG van het ministerie van Justitie & Veiligheid zijn dit de volgende onderdelen:

- het onderwerp en de duur van de verwerking;
- de aard en het doel van de verwerking;
- het soort persoonsgegevens en de categorieën van betrokkenen;
- de rechten en verplichtingen van de verwerkingsverantwoordelijke.
- verder dient in de verwerkersovereenkomst te worden bepaald dat de verwerker:
    - de persoonsgegevens alleen verwerkt onder de schriftelijke instructies van de verwerkingsverantwoordelijke, onder andere voor wat betreft de doorgifte van persoonsgegevens aan een derde land of een internationale organisatie (tenzij deze daartoe wettelijk is verplicht);
    - waarborgt dat de toegang tot die gegevens is beperkt tot gemachtigde personen. Deze personen moeten gebonden zijn aan geheimhouding op grond van een overeenkomst of een wettelijke verplichting;
    - minimaal hetzelfde niveau van beveiliging van de persoonsgegevens hanteert als de verwerkingsverantwoordelijke;
    - de verwerkingsverantwoordelijke alle mogelijke ondersteuning biedt bij het nakomen van diens verplichtingen met het oog op de beantwoording van verzoeken rondom de rechten van betrokkenen;
    - de verwerkingsverantwoordelijke bijstaat bij het nakomen van diens verplichtingen op het gebied van de beveiliging van persoonsgegevens en de meldplicht datalekken;
    - na beëindiging van de overeenkomst de in opdracht van de verwerkingsverantwoordelijke verwerkte persoonsgegevens wist of teruggeeft, en bestaande kopieën verwijdert;
    - de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om aantoonbaar te maken dat de verplichtingen op grond van de Verordening rondom het inzetten van een verwerker worden nageleefd en die nodig is om audits mogelijk te maken;
    - afspraken met betrekking tot sub-verwerkers maakt.

Let op: de wet schrijft niet voor dat de verwerkersovereenkomst een afzonderlijke overeenkomst moet zijn. Vaak wordt het opgenomen in (online ter beschikking gestelde) licentie- of algemene voorwaarden.

Branche-kleuring:
Overeenkomsten zijn algemeen maar het maatwerk zit hem in vooral in het beschrijven van de verwerking waar het om gaat, de toestemmingsprocedure bij het inzetten van sub verwerkers, de vraag waar de data worden opgeslagen, de bewaartermijnen, en de maatregelen die specifiek voor de betreffende verwerking worden afgesproken inclusief controle op de naleving daarvan.

Voorbeelden van derde verwerkingen zijn: de verificatie van ID bewijzen, gebruik van online software voor recruitment of salarisadministratie, planning of tijdregistratie, gps-tracking, et cetera.

Hulpmiddelen:
Templates: ABU, NBBU, AVG Flex Oké

Beschrijving normpunt:

6.2. De organisatie evalueert periodiek de prestaties en compliance van derde partijen onder andere door middel van opgevraagde informatie, bezoeken of audits.

Significantie normpunt:
Laag

AVG:
Artt. 28.3h en 32

Onderbouwing:

De organisatie toont aan dat de afspraken gemaakt in de overeenkomsten worden nageleefd en dat de ingeschakelde verwerker voldoende garanties biedt met betrekking tot het toepassen van passende maatregelen.

Toelichting:
Een organisatie moet kunnen aantonen dat deze de AVG naleeft. Dit doet zij door toe te zien op de uitvoering van de verwerkersovereenkomst of eventueel overeenkomsten in het kader van gezamenlijke verwerkingsverantwoordelijkheid. Dit kan onder andere gedaan worden door middel van opgevraagde informatie, door bezoeken, door (in- of externe) audits of door het opvragen en laten onderhouden van kwaliteitskeurmerken en/of certificaten.

Branche-kleuring:
-

Hulpmiddelen:
- ISO27001, norm met aandacht voor informatiebeveiliging
- Third party memorandum: externe privacy audit op basis van bijvoorbeeld het normenkader van https://www.norea.nl/download/?id=4160 of ISAE 3000
- AVG Garant keurmerk

Beschrijving normpunt:

6.3. Daar waar de organisatie een gezamenlijke verwerkingsverantwoordelijke is, heeft zij met de andere verwerkersverantwoordelijken afspraken gemaakt overeenkomstig de bepalingen in de AVG.

Significantie normpunt:
Laag

AVG:
Art. 26

Onderbouwing:
Als de organisatie een gezamenlijke verwerkingsverantwoordelijke is toont zij aan dat zij met de andere partij afspraken gemaakt heeft over de verantwoordelijkheidsverdeling.

Toelichting:
Het kan zijn dat de organisatie een gezamenlijke verwerkingsverantwoordelijke is (als ze gezamenlijk doel en middelen vaststellen). In dat geval moeten er tussen beide organisaties afspraken gemaakt worden over de verantwoordelijkheidsverdeling met name met betrekking tot de uitoefening van de rechten van de betrokkenen en de informatieverstrekking aan betrokkenen.

Branche-kleuring:
Het komt niet snel voor dat er gezamenlijk doel en middelen worden vastgesteld (gezamenlijk verantwoordelijkheid). Toch kan het wel voorkomen, denk aan de situatie waarbij een organisatie zijn juridisch werkgeverschap uitbesteed aan een back-office payroll organisatie.

Hulpmiddelen:
-

7. Incident- en datalekregistratie

Beschrijving normpunt:
De organisatie heeft en onderhoudt afspraken en een register om incidenten en datalekken registreren, te evalueren en zo nodig (tijdig) te melden bij de AP en de betrokkene(n) te informeren.

Significantie normpunt:
Hoog

AVG:
Artt. 33 en 34

Onderbouwing:
De organisatie toont aan dat er interne afspraken (‘datalekprotocol’) bestaan die borgen dat (potentiële) datalekken intern worden gemeld, in een register worden vastgelegd conform de vereisten uit de AVG, (tijdig) worden afgehandeld en dat er maatregelen worden genomen om dergelijke datalekken in de toekomst te voorkomen.

Toelichting:
Datalekken moeten als deze privacy risico's opleveren tijdig (zonder onredelijke vertraging en uiterlijk 72 uur na bekend worden van de inbreuk) aan de toezichthouder gemeld worden, en indien het grote privacy risico's betreft aan betrokkenen.

Daarnaast moeten datalekken worden vastgelegd waarbij het gaat om: de aard en omstandigheden van het datalek, de gevolgen en de genomen maatregelen. Dit geldt niet alleen voor de datalekken bij de eigen organisatie (Verwerkingsverantwoordelijke) maar ook voor die bij de ingeschakelde Verwerkers. Verwerkers hebben de verplichting datalekken onverwijld te melden aan de Verwerkingsverantwoordelijke.

In het register staan zowel de datalekken die hebben geleid tot een melding aan de AP als ook de datalekken die naar de mening van de organisatie niet gemeld hoefden te worden.

In het register zijn opgenomen de elementen om de mate van het risico van het datalek vast te stellen (o.a. aard incident, aard, gevoeligheid en omvang betrokken gegevens, de ernst van de gevolgen voor betrokkenen en het aantal betrokkenen), de inschatting van het risico, het besluit al of niet te melden en/of te informeren en de genomen maatregelen om de gevolgen te herstellen en in de toekomst te voorkomen.

Om datalekken tijdig gemeld te krijgen is het van belang om medewerkers goed te informeren over wat datalekken zijn en bij wie ze deze moeten melden.

Branche-kleuring:
Voorbeelden van datalekken: verzenden van loonspecificatie of uitzendbevestiging naar verkeerde uitzendkracht of klant, een klant krijgt in een portal inzage in persoonsgegevens van anderen, het opslaan van documenten onder een verkeerde naam, het verstrekken van bijzondere persoonsgegevens aan klanten of systemen die gehackt worden waardoor persoonsgegevens niet meer beschikbaar zijn et cetera.

Hulpmiddelen:
Templates: ABU, NBBU, AVG Flex Ok.

8. Kennis & competentie medewerkers

Beschrijving normpunt:

De organisatie draagt er zorg voor dat medewerkers op de hoogte zijn én blijven van de relevante privacyregels en beschikken over de juiste privacy competenties, - kennis en veiligheidsbewustzijn waarbij rekening wordt gehouden met de aard van de functies en werkzaamheden.

Significantie normpunt:
Laag

AVG:
Artt. 24, 39 1b, 32.1

Onderbouwing:
Uit het opleidingsbeleid van de ondernemer moet blijken dat medewerkers die over meer kennis en competenties moeten beschikken dan de basiskennis in de gelegenheid worden gesteld deze te verwerven. De organisatie dient bovendien een overzicht bij te houden van de door de medewerkers gevolgde trainingen, instructies of andere relevante activiteiten.

Toelichting:
Kennis en competenties kunnen worden vergroot door middel van E-learning, werkinstructies, presentaties, trainingen et cetera.

Branche-kleuring:
De eindtermen van de SEU[13] omschrijven dat "de medewerker weet om te gaan met privacygevoelige informatie". Kennis van de basisbeginselen van de privacywetgeving is dus een vereiste. De SEU biedt examens voor zowel Uitzendprofessionals als Backoffice Professionals.

Hulpmiddelen:
Artra AVG e-learning, https://www.artra.nl/opleiding/avg-oke-e-learning/
ABU Privacy Challenge App

9. Monitoren privacy ontwikkeling

Beschrijving normpunt:

De organisatie zorgt ervoor dat ze geïnformeerd blijft over van belang zijnde privacy-ontwikkelingen zoals wet- en regelgeving, relevante jurisprudentie en technologische ontwikkelingen en handelt op basis van risico's hierop.

Significantie normpunt:
Laag

AVG:
Artt. 24.1., 32.1.

Onderbouwing:
De organisatie toont middelen aan waarmee zij op de hoogte blijft van relevante ontwikkelingen en jurisprudentie bijvoorbeeld door lidmaatschappen, nieuwsbrieven, communicatie met leveranciers, et cetera.

Toelichting:
De organisatie moet zijn privacy risico's managen waarbij ze rekening houdt met omstandigheden en ontwikkelingen waaronder die op het gebied van recht en techniek. Dit geldt voor nieuwe verwerkingen maar ook voor bestaande verwerkingen. Minimaal 1 maal per jaarmoet de organisatie nagaan of genomen maatregelen nog afdoende zijn.

Branche-kleuring:

[13] Stichting Examens Uitzendbranche (SEU) organiseert examens voor medewerkers van uitzend- en payrll, plus payrollorganisaties.

Informatie over (technische en juridische) ontwikkelingen kunnen verkregen worden van brancheorganisaties (ABU, NBBU, BOVIB, VVDN), leveranciers (advocaten, softwarebureaus, marketing), nieuwsbrieven etc..

Hulpmiddelen:
Nieuwsbrieven/websites ABU, NBBU, BOVIB.
Website Stichting AVG Garant.
Nieuwsbrief AP.
Via FG.

10. Uitvoeren rechten betrokkenen

Beschrijving normpunt:
De organisatie zorgt ervoor dat ze in staat is om op verzoeken van betrokkenen om hun rechten uit te voeren, tijdig en adequaat te reageren. Het gaat hierbij om de volgende rechten: inzage (art 15 AVG), rectificatie (art 16 AVG), wissing (art 17 AVG), beperking van de verwerking (art 18 AVG), kennisgeving (art 19 AVG) of overdraagbaarheid van hun gegevens (art 20 AVG), recht van bezwaar (art 21 AVG), recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking (art 22 AVG) gebaseerde besluit.

Significantie normpunt:
Hoog

AVG:
Artt. 12, lid 3, 15-22

Onderbouwing:
De organisatie toont aan dat er interne afspraken, protocollen of procedures zijn op basis waarvan de relevante acties ondernomen worden om de verzoeken van betrokkenen al of niet te honoreren. Voor alle verzoeken geldt dat de verzoeker geïdentificeerd dient te worden om het verzoek in behandeling te kunnen nemen en dat ze binnen de gestelde termijnen op een veilige wijze worden afgehandeld. In dit kader is vastlegging van verzoek en afhandeling nodig (bijvoorbeeld in een verzoekenregister).

In het "privacy-statement (zie normpunt 14)" dienen betrokkenen gewezen te worden op hun rechten en de contactgegevens van de verwerkingsverantwoordelijke.

Toelichting:
Op verzoeken van betrokkenen dient onverwijld en in ieder geval binnen 1 maand gereageerd te worden. De verwerkingsverantwoordelijke dient de identiteit van de verzoeker vast te stellen.

Het wissen van persoonsgegevens op verzoek van de betrokkene kan niet als het bewaren van de gegevens langer vereist is bijvoorbeeld omdat er nog een fiscale bewaarplicht geldt. Wissen kan wel als de betrokkenen zijn toestemming intrekt en er geen andere rechtsgronden gelden.

Branche-kleuring:
-

Hulpmiddelen:
https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen.
Notitie over recht van overdraagbaarheid: ABU.
Informeer bij uw softwareleverancier naar ondersteunende functionaliteiten.

11. Privacy by design & by default

Beschrijving normpunt:
De organisatie houdt bij het ontwerpen en wijzigen van systemen en applicaties rekening met de privacy beginselen en -risico's (privacy by design en by default).

Significantie normpunt:
Laag

AVG:
Art. 25

Onderbouwing:
Stel vast of er procedures of een aanpak aanwezig is om bij nieuwe en aangepaste verwerkingen rekening te houden met privacyrisico's. Maatregelen die hierbij genomen kunnen worden zijn: pseudonimiserende maatregelen, dataminimalisatie, en privacy vriendelijk inrichten van standaarden.

Toelichting:
Dit principe kan ook worden toegepast bij de aanschaf van nieuwe software en bij het aanpassen van bestaande systemen om ze te laten voldoen aan de AVG; het laatste wordt ook wel privacy by re-design genoemd.

Branche-kleuring:
Veel geleverde software in de branche houdt rekening met de AVG. Denk aan het – na invoer – niet langer zichtbaar zijn van BSN; het (standaard) instellen van bewaartermijnen, of het verwijderen van een kopie ID-bewijs vier weken na inschrijving.

Hulpmiddelen:
Handleiding AVG (5.7): Ministerie van J&V
Privacy by design framework: https://www.privacycompany.eu/blog-privacy-by-design-raamwerk/
Handleiding Privacy by design: cip-overheid.nl

2. LEVENSCYCLUS

2.1. Verzamelen

12. Rechtmatige verwerking

Beschrijving normpunt:

De organisatie heeft vastgesteld dat de verwerkingen rechtmatig zijn en in het geval van bijzondere persoonsgegevens en persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten voldoen aan één van de uitzonderingssituaties. En dat het Burgerservicenummer (BSN) uitsluitend wordt verwerkt conform de in de wet beschreven situaties.

Significantie normpunt:
Hoog

AVG:
Artt. 5, 6, 9,10 en 87

UAVG:
Artt. 22-33, 46

Onderbouwing:
De organisatie toont aan de verwerkingen rechtmatig zijn (een geldige grondslag hebben), Voor de hand ligt het dat deze grondslagen zijn opgenomen in het verwerkingenregister. Daarnaast kan als onderbouwing gelden de informatie die is opgenomen in het privacybeleid of de privacy-statements waarin de grondslagen zijn vermeld.

Toelichting:
Rechtmatige grondslagen zijn:
- toestemming van betrokkenen;
- noodzakelijk voor de uitvoering van de overeenkomst;
- noodzakelijk om te voldoen aan een wettelijke verplichting;
- noodzakelijk om vitale belangen van betrokkene of een ander te beschermen;
- noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de Verwerkingsverantwoordelijke of een derde;
- noodzakelijk voor de bescherming van de vitale belangen van de betrokkenen.

De verwerking van bijzondere persoonsgegevens is alleen mogelijk op grond van de wet of een wettelijke uitzondering. In de Uitvoeringswet AVG zijn uitzonderingen opgenomen voor de verwerking van bijzondere persoonsgegevens.

De verwerking van strafrechtelijke gegevens is zonder toestemming van de AP niet toegestaan.

Branche-kleuring:
Meest voorkomende grondslagen zijn de overeenkomst (bijv. dienstverbanden), wettelijke verplichting (bijv. delen gegevens met UWV of pensioenfonds) en het gerechtvaardigd belang (bijv. het delen van gegevens met opdrachtgevers het kader van inlenersaansprakelijkheid). Toestemming ligt minder voor de hand in een relatie tussen een werknemer en werkgever aangezien de toestemming altijd vrijelijk gegeven moet worden.

Soms zijn bij verwerkingen meerdere grondslagen mogelijk. Bij sollicitaties komen de grondslagen overeenkomst, toestemming en gerechtvaardigd belang voor. De organisatie dient zijn keuze te onderbouwen. Bovendien gelden er verschillende eisen waar de organisatie rekening mee moet houden.

Voorbeelden van verwerkingen van het BSN op grond van de wet: BSN bij indiensttreding of in communicatie met UWV en belastingdienst; ziekmelding aan arbodienst of UWV;

gezondheidsgegevens t.b.v. pensioen of re-integratie; biometrische gegevens t.b.v. unieke identificatie in het kader van authenticatie of beveiliging.

Het verwerken van een VOG is geen strafrechtelijk gegeven.

Hulpmiddelen:
Handleiding AVG, hoofdstuk 4: ministerie van J&V
https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/verstrekken-van-persoonsgegevens

13. Toestemming

Beschrijving normpunt:
Als de verwerking is gebaseerd op toestemming van de betrokkene, moet de organisatie hierbij aantonen dat de toestemming rechtmatig is.

Significantie normpunt:
Hoog

AVG:
Artt. 4, 7 (en 8)

Onderbouwing:
Voor de verwerkingen waarvoor de organisatie de grondslag toestemming heeft gebruikt, moet hij voor deze verwerkingen kunnen aantonen hoe de betrokkene is geïnformeerd, op welke wijze de toestemming is gegeven, wanneer deze is gegeven en – voor zover van toepassing - wanneer deze ingetrokken is.

Toelichting:
Voor een rechtmatige toestemming geldt:
- dat toestemming actief is verstrekt;
- dat toestemming vrijelijk is gegeven;
- dat betrokkenen duidelijk geïnformeerd zijn, en
- dat toestemming even makkelijk kan worden ingetrokken als gegeven.

Branche-kleuring:
In de relatie tussen sollicitant/werknemer en werkgever is toestemming zelden toegestaan. Voorbeelden van toestemming die wel mogelijk zijn: toestemming om bij einde inschrijving deze te verlengen, toestemming om foto's te verwerken anders dan voor identificatie, toestemming voor het checken van referenties of toestemming om nieuwsbrieven te verzenden aan prospects. Ook kan na een sollicitatie toestemming gegeven worden om gegevens verder te verwerken in het kader van bemiddeling naar andere functies.

Hulpmiddelen:
Handleiding AVG, hoofdstuk 4: ministerie van J&V.

14. Informatie betrokkenen

Beschrijving normpunt:

14.1. De organisatie informeert betrokkenen over de verwerking van hun persoonsgegevens waarbij tenminste de verplichte onderdelen (zie toelichting) uit de AVG zijn opgenomen ("privacystatement").

Significantie normpunt:
Hoog

AVG:
Artt. 12, 13 en 14.

Onderbouwing:
De organisatie toont - bijvoorbeeld aan de hand van een procedure - aan dat deze informatie verstrekt wordt, welke "privacy-statements" er zijn, en dat deze voldoen aan de eisen van de AVG.

Toelichting:
De informatie dient volgens de AVG de volgende onderwerpen te bevatten:
- de identiteitsgegevens van de organisatie;
- indien van toepassing de contactgegevens van de FG;
- de doeleinden van de verwerking;
- de gerechtvaardigde belangen als daar gebruik van gemaakt wordt;
- de derde ontvangers;
- de waarborgen als gegevens buiten de EER worden verstrekt:
- de bewaartermijnen of de criteria ter bepaling van die termijnen;
- de rechten van betrokkenen;
- de maatregelen bij profilering.

Indien de persoonsgegevens niet van betrokkenen zelf zijn ontvangen informeert de organisatie betrokkenen ook over de betrokken categorieën van persoonsgegevens.

Branche-kleuring:
Informatie kan schriftelijk of via websites verstrekt worden, al of niet onder de noemer van privacy-statement. Belangrijke groepen van betrokkenen zijn: sollicitanten, flexwerkers, bemiddelde ZZP'ers, klanten en leveranciers en eigen medewerkers.

Soms worden persoonsgegevens van derden ontvangen. Denk aan inleners die zelf de werving hebben gedaan en gegevens doorgeven aan de payrollorganisatie. Of aan de situatie dat organisaties profielen van Linkedin halen of van het UWV ontvangen. In die gevallen moeten betrokkenen hierover geïnformeerd worden.

Hulpmiddelen:
Templates: ABU, NBBU

Beschrijving normpunt:

14.2. De organisatie zorgt ervoor dat deze informatie goed leesbaar (beknopt, begrijpelijk, in duidelijke en eenvoudige taal) is opgesteld, tijdig aan betrokkenen is verstrekt, en gemakkelijk toegankelijk is.

Significantie normpunt:
Laag

AVG:
Art. 12

Onderbouwing:
De ondernemer toont aan dat de informatie toegankelijk is, en dat de tekst vóór verstrekking kenbaar wordt gemaakt aan betrokkenen. Verder is van belang dat de tekst goed leesbaar is voor de doelgroep.

Toelichting:
Op grond van de AVG moeten betrokkenen voorafgaand aan de verwerking geïnformeerd worden. Verder geldt dat de informatie beknopt, transparant, in duidelijke en eenvoudige taal en in begrijpelijk en gemakkelijk toegankelijke vorm moet worden aangeboden.

Branche-kleuring:
- In veel gevallen worden persoonsgegevens online verzameld. In die gevallen worden de betrokkenen meestal geïnformeerd door middel van een privacystatement (een link meestal in de footer of in het scherm waarin je kunt solliciteren).
- Indien persoonsgegevens offline worden verstrekt (bijvoorbeeld als werkzoekenden zich op een vestiging inschrijven voor bemiddeling naar werk) dient de organisatie een procedure te hebben om de informatie ter beschikking te stellen.
- Als organisaties van anderstaligen persoonsgegevens verwerken dient daar rekening mee gehouden te worden.

Hulpmiddelen:
- Templates: ABU, NBBU
- Richtsnoeren inzake transparantie, EDPB (11 april 2018)

15. Dataminimalisatie

Beschrijving normpunt:
De organisatie verzamelt en verwerkt alleen die persoonsgegevens die noodzakelijk zijn voor het doel (toereikend en ter zake dienend zijn).

Significantie normpunt:
Hoog

AVG:
Art. 5.1c

Onderbouwing:
De organisatie toont aan dat ze zich houdt aan het beginsel van dataminimalisatie. Dit beginsel kan opgenomen zijn in het privacybeleid en is te toetsen door vast te stellen dat de persoonsgegevens die in het verwerkingenregister zijn opgenomen niet bovenmatig zijn voor het doel waarvoor ze verzameld zijn. Het beginsel van dataminimalisatie is niet alleen van toepassing op het verzamelen van gegevens maar ook op de doorgifte van persoonsgegevens.

Toelichting:
-

Branche-kleuring:
Bij elke verwerking van persoonsgegevens is dataminimalisatie aan de orde. Voorbeelden: bij een inschrijving van een werkzoekende is het niet nodig een bankrekeningnummer op te slaan. Voor het verstrekken van CV's aan opdrachtgevers is het niet noodzakelijk om naam en/of contactgegevens op te nemen.

Hulpmiddelen:
-

2.2. Gebruik, delen en opslaan

16. Doelbinding

Beschrijving normpunt:
De organisatie draagt er zorg voor dat persoonsgegevens uitsluitend voor het doel waarvoor ze verzameld zijn (zoals dat gecommuniceerd is) worden gebruikt of daarmee verenigbaar zijn. Worden gegevens toch voor andere doeleinden gebruikt dan zal de organisatie hiervoor de toestemming van betrokkenen moeten vragen (zie verder normpunt 13).

Significantie normpunt:
Hoog

AVG:
Art. 5.1b

Onderbouwing:
De organisatie houdt zich aan doelbinding. Dit uitgangspunt is vaak te vinden in het privacy-beleid. De doelen zijn omschreven in het verwerkingenregister. Te toetsen door vast te stellen dat niet gebleken is dat persoonsgegevens voor andere doelen worden gebruikt (negative assurance).

Toelichting:
Verwerking voor andere doeleinden is alleen mogelijk als dit verenigbaar is met de oorspronkelijke doeleinden. Op grond van de AVG kan dit bijvoorbeeld van toepassing zijn als gegevens verder worden verwerkt voor statistische doeleinden.

Bij het vaststellen of er sprake is van verenigbaarheid moet de organisatie rekening houden met:
- een eventuele koppeling tussen de doeleinden,
- het kader waarin gegevens zijn verzameld,
- wat betrokkenen in redelijkheid mogen verwachten rekening houdend met hun relatie tot de organisatie,
- de aard van de persoonsgegevens,
- de gevolgen van de verwerking,
- en de veiligheidsmaatregelen die worden genomen.

Branche-kleuring:
-

Hulpmiddelen:
-

17. Verstrekking aan derden

Beschrijving normpunt:
Als de organisatie persoonsgegevens aan derden verstrekt draagt hij er zorg voor dat: a) hij hiervoor een geldende grondslag heeft; b) de verstrekking plaatsvindt in het kader van het doel van de verwerking; c) hij betrokkenen hierover informeert, en d) deze verstrekkingen zijn opgenomen in het verwerkingenregister.

Significantie normpunt:
Laag

AVG:
Artt. 5.1b, 6, 13.3, 30.1d

Onderbouwing:
Dit uitgangspunt is meestal verwoord in het privacy beleid en/of het privacy-statement. In het register is vastgelegd aan welke ontvangers persoonsgegevens worden verstrekt. Op dit punt kan alleen een 'negative assurance' verstrekt worden eruit bestaande dat tijdens de audit niet is vastgesteld dat er persoonsgegevens onrechtmatig aan derden zijn verstrekt.

Toelichting:
-

Branche-kleuring:
-

Hulpmiddelen:
-

2.3. Archiveren en wissen

18. Bewaartermijnen

Beschrijving normpunt:
De organisatie heeft en onderhoudt een overzicht van bewaartermijnen en draagt er zorg voor dat deze wordt nageleefd. Na afloop van de termijnen dienen persoonsgegevens verwijderd of anoniem gemaakt te worden.

Significantie normpunt:
Hoog

AVG:
Artt. 5.1e, 89.1

Onderbouwing:
Bewaartermijnen zijn meestal opgenomen in het verwerkingenregister. Daarnaast wordt er in de privacy-statements of het beleid en/of in andere documenten naar verwezen. Heeft de organisatie meerdere overzichten, dan moet de consistentie worden nagegaan.

Bij de audit wordt nagegaan of termijnen ook daadwerkelijk gehandhaafd worden (door middel van het controleren van systeeminstellingen en het nemen van een steekproef). Gegevens kunnen worden gewist of worden geanonimiseerd.

Toelichting:
Op het moment van invoeren van de AVG hielden nog niet alle systemen voldoende rekening met bewaartermijnen. Aanpassing van de systemen vraagt tijd, maar door een privacy by design aanpak zal dit op termijn goed ingeregeld worden.

Branche-kleuring:
Overzicht bewaartermijnen: ABU, NBBU

Hulpmiddelen:
- Het oude vrijstellingsbesluit WBP bevat nog altijd relevante termijnen.
- Ga ook bij softwareleverancier na of er bewaarfunctionaliteiten zijn.
- Maak onderscheid tussen gebruiks- en archieffase en pas door toegang op aan.

2.4. Overstijgende maatregelen

19. Passende beveiligingsmaatregelen

Beschrijving normpunt:

De organisatie neemt passende organisatorische en technische maatregelen om een op het risico afgestemd beveiligingsniveau van persoonsgegevens te waarborgen.

Significantie normpunt:
Hoog

AVG:
Artt. 24,30, 32

Onderbouwing:
De organisatie maakt inzichtelijk wat de belangrijkste risico's zijn voor zijn informatiesystemen en welke maatregelen hij heeft genomen om deze risico's af te dekken.

Toelichting:
Op grond van de AVG moet, indien mogelijk, in het verwerkingenregister een algemene beschrijving van de beveiligingsmaatregelen opgenomen zijn. De organisatie kan bij dit punt van deze beschrijving gebruik maken, maar meestal zullen deze maatregelen slechts in abstracte termen geformuleerd zijn. Aanvullend kunnen maatregelen opgenomen zijn in een informatiebeveiligingsplan.

Branche-kleuring:
-

Hulpmiddelen:
Maatregelenlijst ISO 27001/NEN 7510
Overzicht beveiligingsmaatregelen: ABU, AVG Flex Oké
Richtsnoeren Beveiliging van persoonsgegevens (par. 3.2): Autoriteit Persoonsgegevens
https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

20. Toegangsrechten en Authenticatie

Beschrijving normpunt:
De organisatie heeft en onderhoudt procedures om toegangsrechten te beheren waarbij gebruikers geauthenticeerd worden bijvoorbeeld door gebruikersnaam en wachtwoord.

Significantie normpunt:
Hoog

AVG:
Artt. 5.1f, 32

Onderbouwing:
De organisatie toont aan dat er autorisatieschema's worden gebruikt en beheerd (bijvoorbeeld op basis van rollen). Het authenticeren en inloggen op systemen vindt plaats op basis van een passend wachtwoordbeleid (daar waar nodig en passend met gebruik van twee-factor authenticatie/2FA).

Toelichting:
Toegang tot systemen dient verstrekt te worden op basis van het need-to-know principe en toegang dient vastgelegd en gecontroleerd te worden. Dit om gegevens vertrouwelijk te houden en te voorkomen dat onrechtmatige toegang leidt tot inbreuken op de beveiliging.

Hierbij moet rekening gehouden worden met specifieke risico's. Bij toegang op afstand (denk aan thuiswerken of werken in de cloud) ligt gebruik van 2FA voor de hand.

Branche-kleuring:
Er wordt veel gebruik gemaakt van cloud-software ten behoeve van sollicitaties, inzage in persoonlijke dossiers, planning en tijdsregistratie. Voor toegang tot deze systemen ligt 2FA voor de hand.

Hulpmiddelen:
Factsheet 2FA: https://www.ncsc.nl/actueel/factsheets/factsheet-gebruik-tweefactorauthenticatie.html: Nationaal Cyber Security Centrum.

21. Juist houden gegevens

Beschrijving normpunt:
De organisatie heeft procedures geïmplementeerd om er zorg voor te dragen dat gegevens juist en accuraat worden verzameld en up to date worden gehouden.

Significantie normpunt:
Laag

AVG:
Art. 5.1d

Onderbouwing:
De organisatie toont procedures, instructies of systeembeschrijvingen aan waaruit dit proces blijkt inclusief de controle op de naleving.

Toelichting:
De organisatie kan dit o.a. doen door het jaarlijks om herbevestiging van data te vragen en/of via portals mogelijkheden te bieden data zelf te laten onderhouden door betrokkenen.

Branche-kleuring:
Te denken valt aan wijzigingsrechten in portals of aan periodieke mails naar ingeschrevenen.

Hulpmiddelen:
-

3. MONITORING EN EVALUATIE

22. Monitoring en evaluatie

Beschrijving normpunt:

De organisatie beoordeelt (periodiek) de operationele effectiviteit van privacy maatregelen en haar beleid.

Significantie normpunt:
Hoog

AVG:
Artt. 24, 32

Onderbouwing:
De organisatie toont middelen van controle en evaluatie aan. Denk aan interne en externe audits, aanwezigheidslijsten trainingen, klachtenrapportages, rapportages van de Functionaris Gegevensbescherming, et cetera. Doel moet zijn dat monitoring leidt tot herstel van tekortkomingen, continue verbetering en aanpassing van het beleid.

Toelichting:
In de wet staat dat de ondernemer passende maatregelen moet nemen en deze evalueert en indien nodig actualiseert.

Branche-kleuring:
-

Hulpmiddelen:
-

Bijlage 1 Wet- en regelgeving

- Algemene Verordening Gegevensbescherming (2016/679, 27 april 2016), voor inhoudsopgave zie hieronder.
- U-AVG (uitvoeringswet AVG) 16 mei 2018.

Inhoudsopgave AVG

72 Procedure
73 Voorzitter
74 Taken van de voorzitter
75 Secretariaat
76 Vertrouwelijkheid

VIII Beroep, aansprakelijkheid en sancties

77 Recht om klacht in te dienen bij een toezichthoudende autoriteit
78 Recht om een doeltreffende voorziening in rechte in te stellen tegen een toezichthoudende autoriteit
79 Recht om een doeltreffende voorziening in rechte in te stellen tegen een verwerkingsverantwoordelijke of een verwerker
80 Vertegenwoordiging van betrokkenen
81 Schorsing van de procedure
82 Recht op schadevergoeding en aansprakelijkheid
83 Algemene voorwaarden voor het opleggen van administratieve geldboeten
84 Sancties

IX Bepalingen in verband met specifieke situaties op het gebied van gegevensverwerking

85 Verwerking en vrijheid van meningsuiting en van informatie
86 Verwerking en recht van toegang van het publiek tot officiële documenten
87 Verwerking van het nationaal identificatienummer
88 Verwerking in het kader van de arbeidsverhouding
89 Waarborgen en afwijkingen in verband met verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden
90 Geheimhoudingsplicht
91 Bestaande gegevensbeschermingsregels van kerken en religieuze verenigingen

X Gedelegeerde handelingen en uitvoeringshandelingen

92 Uitoefening van de bevoegdheidsdelegatie
93 Comitéprocedure

XI Slotbepalingen

94 Intrekking van Richtlijn 95/46/EG
95 Verhouding tot Richtlijn 2002/58/EG
96 Verhouding tot eerder gesloten overeenkomsten
97 Commissieverslagen
98 Toetsing van andere Unierechtshandelingen inzake gegevensbescherming
99 Inwerkingtreding en toepassing

AVG-guidelines

De AP publiceert samen met de andere Europese privacytoezichthouders guidelines die bepaalde onderwerpen uit de AVG verduidelijken. Op https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/avg-guidelines is altijd de actuele status van deze guidelines te vinden.

Bijlage 2 Definities

	Begrip	Definitie	Vindplaats
A	accreditation	an attestation13 by a national accreditation body and/or by a supervisory authority, that a certification body14 is qualified to carry out certification pursuant to Article 42 and 43 GDPR, taking into account ISO/IEC 17065/2012 and the additional requirements established by the supervisory authority and or by the Board;	4/2018, 4 december 2018, on the accreditation of certification bodies, EDPB
	anonimisatie	proces waarbij persoonsgegevens onomkeerbaar worden veranderd, zodanig dat de betreffende persoon niet langer kan worden geïdentificeerd, direct of indirect, hetzij door de beheerder van de persoonsgegevens alleen, hetzij in samenwerking met een andere partij;	ISO27001/9001
	AP	Autoriteit Persoonsgegevens;	UAVG, art. 6
	AVG	Algemene Verordening Gegevensbescherming (de Verordening);	UAVG, art. 1
	audit	Systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van auditbewijs materiaal en het objectief beoordelen daarvan om vast te stellen in welke mate aan de auditcriteria wordt voldaan;	ISO27001/9001
	authenticatie	het verschaffen van zekerheid met betrekking tot de juistheid van een geclaimde karakteristiek;	ISO27001/9001.
	autorisatie	toekennen van bevoegdheden;	ISO27001/9001
B	beheersmaatregel	maatregel waarmee een risico wordt gewijzigd;	ISO27001/9001
	beleid	intenties en richting van een organisatie zoals formeel door haar directie kenbaar gemaakt;	ISO27001/9001
	beoordeling	activiteit die wordt ondernomen om de geschiktheid, toereikendheid en doeltreffendheid van het desbetreffende onderwerp voor het behalen van vastgestelde doelstellingen te bepalen;	ISO27001/9001
	beperking van de verwerking	het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken;	AVG, art. 4 lid 3
	bestand	elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid;	AVG, art. 4 lid 6
	bezwaar (relevant en gemotiveerd)	een bezwaar tegen een ontwerpbesluit over het bestaan van een inbreuk op deze verordening of over de vraag of de	AVG, art. 4 lid 24

		voorgenomen maatregel met betrekking tot de verwerkingsverantwoordelijke of de verwerker strookt met deze verordening, waarin duidelijk de omvang wordt aangetoond van de risico's die het ontwerpbesluit inhoudt voor de grondrechten en de fundamentele vrijheden van betrokkenen en, indien van toepassing, voor het vrije verkeer van persoonsgegevens binnen de Unie;	
	Bijzondere persoonsgegevens	de categorieën van persoonsgegevens zoals, bedoeld in artikel 9, eerste lid, van de verordening;	UAVG, art. 1; AVG art. 9
	bindende bedrijfsvoorschriften	beleid inzake de bescherming van persoonsgegevens dat een op het grondgebied van een lidstaat gevestigde verwerkingsverantwoordelijke of verwerker voert met betrekking tot de doorgifte of reeksen van doorgiften van persoonsgegevens aan een verwerkingsverantwoordelijke of verwerker in een of meer derde landen binnen een concern of een groepering van organisaties die gezamenlijk een economische activiteit uitoefenen;	AVG, art. 4 lid 20
	biometrische gegevens	persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens;	AVG, art. 4 lid 14
C	certification	the assessment and impartial, third party attestation that the fulfilment of certification criteria has been demonstrated;	4/2018, 4 december 2018, on the accreditation of certification bodies, EDPB.
	certification body	a third –party conformity assessment body operating a certification mechanisms;	4/2018, 4 december 2018, on the accreditation of certification bodies, EDPB.
	certification criteria	the criteria against which a certification is performed;	4/2018, 4 december 2018, on the accreditation of certification bodies, EDPB.
	certification scheme	certification system related to specified products, processes and services to which the same specified requirements, specific rules and procedures apply;	4/2018, 4 december 2018, on the accreditation of

			certification bodies, EDPB.
C	concern	een organisatie die zeggenschap uitoefent en de organisaties waarover die zeggenschap wordt uitgeoefend;	AVG, art. 4 lid 19
D	derde	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken;	AVG, art. 4 lid 10
	directie	persoon of groep van personen die een organisatie op het hoogste niveau bestuurt en beheert;	ISO27001/9001.
	DPIA	Data Protection Impact Assessment	AVG, art. 35
	dienst van de informatiemaatschappij	een dienst als gedefinieerd in artikel 1, lid 1, punt b), van Richtlijn (EU) 2015/1535 van het Europees Parlement en de Raad (19);	AVG, art. 4 lid 25
E	EDPB	European Data Protection Board	AVG, art. 68
F	FG	Functionaris Gegevensbescherming	AVG, art. 37
G	gegevens over gezondheid	persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven;	AVG, art. 15
	genetische gegevens	persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon;	AVG, art. 4 lid 13
	grensoverschrijdende verwerking":	a) verwerking van persoonsgegevens in het kader van de activiteiten van vestigingen in meer dan één lidstaat van een verwerkingsverantwoordelijke of een verwerker in de Unie die in meer dan één lidstaat is gevestigd; of b) verwerking van persoonsgegevens in het kader van de activiteiten van één vestiging van een verwerkingsverantwoordelijke of van een verwerker in de Unie, waardoor in meer dan één lidstaat betrokkenen wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden;	AVG, art. 4 lid 23
H	hoofdvestiging	a) met betrekking tot een verwerkingsverantwoordelijke die vestigingen heeft in meer dan één lidstaat, de plaats waar zijn centrale administratie in de Unie is gelegen, tenzij de beslissingen	AVG, art. 4 lid 16

		over de doelstellingen van en de middelen voor de verwerking van persoonsgegevens worden genomen in een andere vestiging van de verwerkingsverantwoordelijke die zich eveneens in de Unie bevindt, en die tevens gemachtigd is die beslissingen uit te voeren, in welk geval de vestiging waar die beslissingen worden genomen als de hoofdvestiging wordt beschouwd; b) met betrekking tot een verwerker die vestigingen in meer dan één lidstaat heeft, de plaats waar zijn centrale administratie in de Unie is gelegen of, wanneer de verwerker geen centrale administratie in de Unie heeft, de vestiging van de verwerker in de Unie waar de voornaamste verwerkingsactiviteiten in het kader van de activiteiten van een vestiging van de verwerker plaatsvinden, voor zover op de verwerker krachtens deze verordening specifieke verplichtingen rusten;	
I	identificatie	bepalen van de identiteit van een persoon of andere entiteit;	ISO27001/9001
	inbreuk in verband met persoonsgegevens (“datalek”)	een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;	AVG, art. 4 lid 12
	informatiebeveiliging	behoud van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie;	ISO27001/9001
	integriteit	eigenschap van nauwkeurigheid en volledigheid;	ISO27001/9001
	internationale organisatie	een organisatie en de daaronder vallende internationaalpubliekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen;	AVG, art. 4 lid 25
L	loggen	voorvallen, activiteiten of het optreden van wijzigingen in een informatiesysteem chronologisch vastleggen;	ISO27001/9001
M	managementsysteem	geheel van samenhangende of elkaar beïnvloedende elementen van een organisatie om een beleid en doelstellingen vast te stellen, alsmede de processen om die doelstellingen te bereiken;	ISO27001/9001
	managementsysteem voor informatiebeveiliging	ISMS, dat deel van een managementsysteem dat op basis van een beoordeling van bedrijfsrisico’s tot doel heeft het vaststellen, implementeren, uitvoeren, controleren, beoordelen, onderhouden en verbeteren van informatiebeveiliging;	ISO27001/9001
O	organisatie	een natuurlijke persoon of rechtspersoon die een economische activiteit uitoefent, ongeacht de rechtsvorm ervan, met	AVG, art. 4 lid 18

		inbegrip van maatschappen en persoonsvennootschappen of verenigingen die regelmatig een economische activiteit uitoefenen;	
	ontvanger	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt. Overheidsinstanties die mogelijk persoonsgegevens ontvangen in het kader van een bijzonder onderzoek overeenkomstig het Unierecht of het lidstatelijk recht gelden echter niet als ontvangers; de verwerking van die gegevens door die overheidsinstanties strookt met de gegevensbeschermingsregels die op het betreffende verwerkingsdoel van toepassing zijn;	AVG, art. 4 lid 9
P	persoonsgegevens	alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.	AVG, art. 4 lid 1
	Persoonsgegevens van strafrechtelijke aard	persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de verordening, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag;	UAVG, art. 1
	profilering	elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;	AVG, art. 4 lid 4
	pseudonimisering	het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart	AVG, art. 4 lid 5

		worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld;	
R	risico	effect van onzekerheid op het behalen van doelstellingen;	ISO27001/9001
	risicomanagement	gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot risico's;	ISO27001/9001
T	toegangsbeveiliging	middel om te bewerkstelligen dat toegang tot bedrijfsmiddelen wordt goedgekeurd en beperkt op basis van de eisen voor bedrijfsvoering en beveiliging;	ISO27001/9001
	toestemming	van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt;	AVG, art. 4 lid 11
	toezichthoudende autoriteit":	een door een lidstaat ingevolge artikel 51 ingestelde onafhankelijke overheidsinstantie;	AVG, art. 4 lid 21
	(betrokken) toezichthoudende autoriteit	een toezichthoudende autoriteit die betrokken is bij de verwerking van persoonsgegevens omdat: a) de verwerkingsverantwoordelijke of de verwerker op het grondgebied van de lidstaat van die toezichthoudende autoriteit is gevestigd; b) de betrokkenen die in de lidstaat van die toezichthoudende autoriteit verblijven, door de verwerking wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden; of c) bij die toezichthoudende autoriteit een klacht is ingediend;	AVG, art. 4 lid 22
V	verificatie	bevestiging dat aan gespecificeerde eisen is voldaan door het verschaffen van objectief bewijs;	ISO27001/9001
	vertegenwoordiger	een in de Unie gevestigde natuurlijke persoon of rechtspersoon die uit hoofde van artikel 27 schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om de verwerkingsverantwoordelijke of de verwerker te vertegenwoordigen in verband met hun respectieve verplichtingen krachtens deze verordening;	AVG, art. 4 lid 17
	vertrouwelijkheid	eigenschap dat informatie niet beschikbaar of niet bekend wordt gemaakt aan onbevoegde personen, entiteiten of processen;	ISO27001/9001
	verwerker	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een	AVG, art. 4 lid 8

		ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;	
	verwerking	een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;	AVG, art. 4 lid 2
	verwerkingsverantwoordelijke	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;	AVG, art. 4 lid 7

Bijlage 3: Kruistabel AVG – AVG Garant

	Kruisverwijzingen (AVG ==> normschema)	
AVG/UAVG		**AVG Garant**
	Hoofdstuk 1	
	Algemene bepalingen	
1	Onderwerp en doelstellingen	
2	Materieel toepassingsgebied	AVG Garant richt zich op organisaties met verwerkingen die onder de AVG vallen.
3	Territoriaal toepassingsgebied	AVG Garant richt zich op Nederlandse organisaties.
4	Definities	De definities uit de AVG en de U-AVG zijn van toepassing verklaard op het normenschema.
	Hoofdstuk 2	
	Beginselen	
5	Beginselen inzake verwerking van persoonsgegevens	12. Rechtmatige verwerking 14. Informatie verwerking persoonsgegevens 15. Dataminimalisatie 16. Doelbinding 17. Verstrekking derden 18. Bewaarbeleid 19. Beveiliging 20. Toegangsrechten 21. Juistheid
6	Rechtmatigheid van de verwerking	3. Verwerkingenregister 12. Rechtmatige verwerkingen 15. Toestemming
7	Voorwaarden voor toestemming	3. Verwerkingenregister 12. Rechtmatige verwerkingen 15. Toestemming
8	Voorwaarden voor de toestemming van kinderen met betrekking tot diensten van de informatiemaatschappij.	N.v.t.

	Kruisverwijzingen (AVG ==> normschema)	
AVG/UAVG		**AVG Garant**
9	Verwerking van bijzondere categorieën van persoonsgegevens (inclusief uitzonderingen in de UAVG hoofdstuk 3)	3. Verwerkingenregister 12. Rechtmatige verwerkingen 13. Toestemming
10	Verwerking van persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten.	3. Verwerkingenregister 12. Rechtmatige verwerkingen 13. Toestemming
11	Verwerking waarvoor identificatie niet is vereist	N.v.t.
	Hoofdstuk 3	
	Rechten van betrokkenen	
12	Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van betrokkenen.	1. Privacybeleid 10. Rechten 14. Informatie verwerking persoonsgegevens 16. Doelbinding 17. Verstrekking derden
13	Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld	1. Privacybeleid 10. Rechten 14. Informatie verwerking persoonsgegevens 16. Doelbinding 17. Verstrekking derden
14	Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen	1. Privacybeleid 10. Rechten 14. Informatie verwerking persoonsgegevens 16. Doelbinding 17. Verstrekking derden
15	Recht van inzage van de betrokkene	1. Privacybeleid 10. Rechten 14. Informatie verwerking persoonsgegevens 16. Doelbinding 17. Verstrekking derden
16	Recht op rectificatie	1. Privacybeleid 10. Rechten 14. Informatie verwerking persoonsgegevens 16. Doelbinding 17. Verstrekking derden

	Kruisverwijzingen (AVG ==> normschema)	
AVG/UAVG		**AVG Garant**
17	Recht op gegevenswissing („recht op vergetelheid”)	1. Privacybeleid 10. Rechten 14. Informatie verwerking persoonsgegevens 16. Doelbinding 17. Verstrekking derden
18	Recht op beperking van de verwerking	1. Privacybeleid 10. Rechten 14. Informatie verwerking persoonsgegevens 16. Doelbinding 17. Verstrekking derden
19	Kennisgevingsplicht inzake rectificatie of wissing van persoonsgegevens of verwerkingsbeperking	1. Privacybeleid 10. Rechten 14. Informatie verwerking persoonsgegevens 16. Doelbinding 17. Verstrekking derden
20	Recht op overdraagbaarheid van gegevens	1. Privacybeleid 10. Rechten 14. Informatie verwerking persoonsgegevens 16. Doelbinding 17. Verstrekking derden
21	Recht van bezwaar	1. Privacybeleid 10. Rechten 14. Informatie verwerking persoonsgegevens 16. Doelbinding 17. Verstrekking derden
22	Geautomatiseerde individuele besluitvorming, waaronder profilering	N.v.t.
23	Beperkingen	N.v.t.
	Hoofdstuk 4	
	Verwerkingsverantwoordelijke en verwerker	
24	Verantwoordelijkheid van de verwerkingsverantwoordelijke (vn 2)	1. Privacybeleid 8. Kennis en competenties 19. Beveiliging 22. Evaluatie

Kruisverwijzingen (AVG ==> normschema)		
AVG/UAVG		**AVG Garant**
25	Gegevensbescherming door ontwerp en door standaardinstellingen	11. Privacy by design
26	Gezamenlijke verwerkingsverantwoordelijken	2. Rollen en verantwoordelijkheden 3. Verwerkingenregister
27	Vertegenwoordigers van niet in de Unie gevestigde verwerkingsverantwoordelijken of verwerkers	n.v.t.
28	Verwerker	2. Rollen en verantwoordelijkheden 3. Verwerkingenregister 4. Verwerkingen buiten de EU
29	Verwerking onder gezag van de verwerkingsverantwoordelijke of de verwerker	2. Rollen en verantwoordelijkheden 3. Verwerkingenregister 4. Verwerkingen buiten de EU 6. Verwerkersovereenkomst
30	Register van de verwerkingsactiviteiten	3. Verwerkingenregister
31	Medewerking met de toezichthoudende autoriteit	6. Verwerkersovereenkomst
32	Beveiliging van de verwerking	8. Kennis en competenties 9. Monitoring 19. Passende beveiliging 20. Toegangsrechten
33	Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit	7. Incidenten en datalekken
34	Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene	7. Incidenten en datalekken
35	Gegevensbeschermingseffectbeoordeling	5. DPIA
36	Voorafgaande raadpleging	5. DPIA
37	Aanwijzing van de Functionaris voor gegevensbescherming	1. Privacybeleid 2. Rollen & verantwoordelijkheden
38	Positie van de Functionaris voor gegevensbescherming	1. Privacybeleid 2. Rollen & verantwoordelijkheden

Kruisverwijzingen (AVG ==> normschema)		
AVG/UAVG		**AVG Garant**
39	Taken van de Functionaris voor gegevensbescherming (vn 2)	1. Privacybeleid 2. Rollen & verantwoordelijkheden 8. Kennis en competenties
	Hoofdstuk 4	
	Doorgiften van persoonsgegevens aan derde landen of internationale organisaties (44 tm 50)	1. Privacybeleid 3. Verwerkingenregister 4. Verwerking buiten de EU 6. Verwerkersovereenkomst
	Hoofdstuk 9	
	Specifieke situaties	
	-	
87	Verwerking van het nationaal identificatienummer (inclusief uitzonderingen in de UAVG hoofdstuk 3)	1. Privacybeleid 3. Verwerkingenregister 12. Rechtmatige verwerkingen

Versiebeheer

Versie	Datum	Wijziging / Actie
0.1	1-9-2019	Eerste concept
0.2	1-3-2019	Versie na interne bespreking
0.3	1-06-2019	Versie na pilot; ingediend RvA
0.4	1-1-2020	Scoremodel, redactie normen 14-22, definities
0.5	1-6-2020	Aanpassing nav eerste bespreking RvA
0.6	8-12-2020	Aanpassing nav tweede bespreking AP