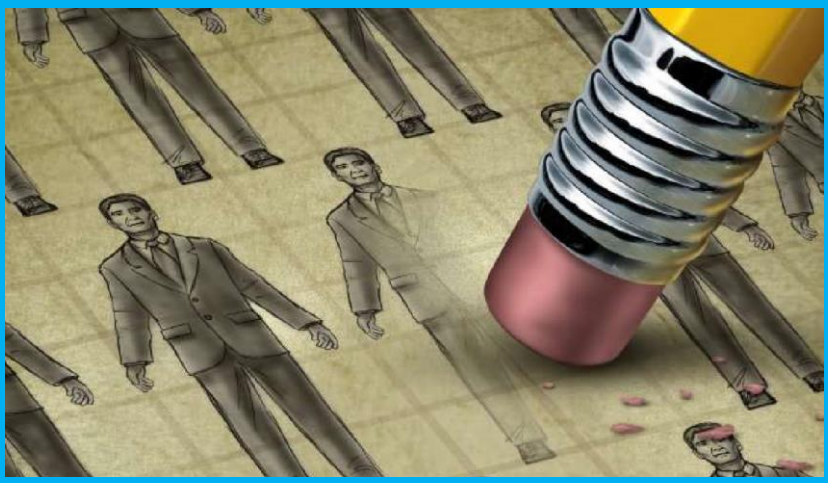
HANDBOEK VOOR DE



PRIVACY OFFICER

Handboek voor de Privacy Officer

Een praktische handleiding

Door Douwe Cnossen
Drs | RC | MBA – CIPM | CTPP | CISSP

Versie 1.0 – oktober 2018
Versie 1.7 – februari 2022

Inhoud

1. Introductie

1.1 Voor wie is dit handboek bedoeld?

Dit handboek is geschreven met één rol in gedachten: de Privacy Officer binnen uw organisatie[1].

Daarnaast is het handboek ook nuttig als u:

- In een vergelijkbare functie verantwoordelijkheid bent voor de Privacy Aanpak, zoals bijv. de Risk & Compliance Officer, medewerker bij de Juridische afdeling, een HR Business partner, of
- Privacy Officer bent of een vergelijkbare rol vervult bij een organisatie die internationaal opereert in landen die niet zijn gereguleerd door de AVG.

Bent u afkomstig van een organisatie die wordt gereguleerd door een andere privacywetgeving, houdt er dan rekening mee dat sommige wettelijke vereisten voor uw organisatie anders zijn dan die in de AVG. Dus hoewel het algemene kader dat we hier beschrijven, nog steeds nuttig is. Onthoud dat sommige van de specifieke regels, zoals wat er bijvoorbeeld in een Privacybeleid moet staan, in dát geval anders kunnen zijn.

1.2 Hoe dit handboek kan helpen

Misschien is de rol van Privacy Officer nieuw binnen uw organisatie en u wilt weten wat de functie-inhoud. Wellicht helpt u uw organisatie met een programma voor Privacy Management en u wilt weten waar u het beste kan beginnen. Of misschien bent u een ervaren Privacy Officer, in een gerenommeerde organisatie, en u wilt gewoon controleren waar de lacunes zich bevinden in uw Privacy programma, die moeten worden opgevuld.

Hoe dan ook, beschouw dit handboek als uw 'To Do'-lijst want er is in ieder geval één ding wat we NIET met dit handboek wilden doen: het wiel opnieuw uitvinden!

Er zijn uitgebreide handleidingen van toezichthouders en adviseurs over de hele wereld over het opzetten, verankeren en onderhouden van programma's voor Privacy Management. In plaats daarvan wilden we u deze beknopte handleiding aanbieden. Enerzijds om u te helpen een vliegende start te maken met uw Privacy Aanpak en anderzijds om u andere bronnen aan te reiken die hun nut in de praktijk bewezen hebben.

[1] Specifiek: opererend binnen de kaders van de Algemene Verordening Gegevensbescherming (AVG), gereguleerd door de Autoriteit Persoonsgegevens (AP).

1.3 Andere bronnen

Bij DATA2TRUST Consultancy (hierna: D2T) ontwikkelen, trainen, publiceren, bloggen en presenteren we over alle dingen die privacy gerelateerd zijn. Dus, net als dit handboek, hebben we een heleboel andere bronnen die we commercieel beschikbaar maken. Te denken valt aan e-Learning-modules, e-Boeken over specifieke onderwerpen, checklists die u kunt gebruiken en sjablonen en templates die u kunt downloaden en aanpassen voor uw eigen organisatie.

Elk van onze trainingen en e-Learning-modules kan worden ingekocht als een zelfstandig item en u kunt natuurlijk ook een pakket samenstellen met de tools die voor u het meest relevant zijn. Dit handboek bevat ook links naar gratis bronnen die verkrijgbaar zijn bij de Autoriteit Persoonsgegevens, de IBD[2], SURFnet[3] en NOREA[4].

[2] Informatiebeveiliginsdienst ondersteunt de VNG - Vereniging van Nederlandse Gemeenten op het gebied van informatiebeveiliging en privacy https://www.informatiebeveiligingsdienst.nl/
[3] Een netwerkorganisatie die een nationaal researchnetwerk ontwikkelt en exploiteert voor onderwijs en onderzoek. Ontwikkelt bovendien diensten als beveiliging en authenticatie.
[4] De beroepsorganisatie van IT-auditors www.norea.nl

2. Wie is de Privacy Officer?

2.1 Rol

De rol van u als Privacy Officer gaat over de ondersteuning van uw organisatie bij het beantwoorden van delicate vragen, zoals: hoe kunnen wij als organisatie maximale waarde uit 'onze' klantgegevens halen, én tegelijkertijd de privacy van de klanten toch goed beschermen?

Niet ieder project is hetzelfde en de impact van nieuwe technologische ontwikkelingen op Privacy wordt steeds complexer. Organisaties begeven zich meer en meer op het pad van data-analytics, huren dataspecialisten in om aan de slag te gaan met Big Data. Zaak voor de Privacy Officer om zich continue te verdiepen in deze nieuwe ontwikkelingen met voortdurend de Privacybescherming in het achterhoofd.

Wil de organisatie u als Privacy Officer en uw team écht als toegevoegde waarde gaan zien dan moet uw rol meer inhouden dan het waarschuwen voor privacy risico's en het verzorgen van trainingsprogramma's voor medewerkers. Uw rol gaat om het stimuleren van een nieuw besef bij het Topmanagement. Namelijk, het besef dat Privacy een nieuwe dimensie toevoegt aan de klantgerichtheid van uw organisatie en dat het vertrouwen in uw Privacy aanpak eerder een 'business' driver is dan een beperking!

Er wordt vaak gezegd dat data het nieuwe goud is. Natuurlijk kun je als organisatie de data 'mijnen', maar ten koste waarvan? De rekenkracht van Big Data belooft veel, maar zonder het vertrouwen van de klanten wordt er geen echte waarde toegevoegd. Zakelijke belangen en klantbelangen staan soms op gespannen voet waar u als Privacy Officer omzichtig mee moet omgegaan.

Neem bijvoorbeeld anonimisering als oplossing voor al uw privacy uitdagingen. Anonimisering wordt vaak voorgesteld als dé oplossing voor privacy kwesties inzake Big Data in combinatie met Marketing & Verkoop respectievelijk Commerciële Ontwikkeling. Maar als het gaat om anonimisering, dan kunt u de AVG alleen toepassen en het projectrisico beoordelen als u eerst de beperkingen van de verschillende anonimiserings-technieken begrijpt. Er zijn legio voorbeelden van informatie die zogenaamd 'geanonimiseerd' was, maar waarbij het 'in-the- end' het toch mogelijk werd om personen te identificeren.

2.2 Taken

De taken van een Privacy Officer gaan verder dan die van de Compliance Officer. Hij of zij is verantwoordelijk voor het ontwerp en beheer van het Privacy Management Programma van de organisatie.

De dagelijkse taken van de Privacy Officer omvatten (niet limitatief):

- Verstrekken van privacy advies aan interne belanghebbenden;
- Zorgen dat het personeel is opgeleid in en op de hoogte is van de privacy verplichtingen;

- Monitoring van privacy risico's, bijv. door audits van operationele gebieden of privacy-effectbeoordelingen van nieuwe projecten uit te voeren of te coördineren;
- Opstellen van privacy documenten, zoals privacy beleid en privacy statements;
- Contact met de Functionaris Gegevensbescherming of Data Protection Officer over meldingen van datalekken, klachten over privacy of belangrijke projecten;
- Behandelen van privacy klachten en informatieverzoeken van het belanghebbenden, en;
- Adviseren over verzoeken om inzage, het corrigeren van persoonsgegevens of verzoeken van derden om toegang te krijgen tot persoonsgegevens.

De taken zijn zowel reactief oplossend (zoals bijvoorbeeld het reageren op externe vragen over privacy of verzoeken om toegang/ correctie) als proactief sturend (zoals bijvoorbeeld Privacy Impact Assessment, Training & Advies en Bewustwordingsprogramma's . . .etc).

2.3 Vaardigheden

Het effectief kunnen implementeren van uw Privacy Aanpak vereist - ongeacht de omvang van de organisatie - vaardigheden, expertise en de juiste middeleninzet.

De Privacy Officer hoeft geen juridische achtergrond te hebben, maar moet minimaal ervaring hebben met het werken in een door regels gestuurde omgeving. Het kunnen omgaan met en het interpreteren van wetgeving is daarbij zeker nuttig. Naar onze mening is materiedeskundigheid vereist maar nog veel belangrijker voor de rol is een verzameling aan zachte vaardigheden, zoals: communicatie, overtuigingskracht en begripsvorming.

Kortom, een succesvolle Privacy Officer is in staat om:
- De bedrijfsactiviteiten en -processen van de organisatie te overzien;
- Een veelvoud aan relaties te onderhouden met stakeholders en senior management, data leveranciers, projectmanagers, evenals personeel in IT, records management, legal, riskmanagement en interne audit/ compliance;
- De privacy aanpak uit te dragen en gedrag te stimuleren, inclusief voortdurende monitoring en beoordeling van de bedrijfsprocessen, en het stimuleren van een *privacy-mindset* bij het topmanagement, zonder zich als een scheidsrechter te moeten gedragen, en
- De privacy aanpak in te zetten als een vehicle om processen, eigenaarschap, klantenrelaties en imago te verbeteren.

De Privacy Officer is bij voorkeur een persoon die door collega's wordt gezien als een specialist en een 'vertrouwenspersoon' voor pragmatisch advies. Voordat u als Privacy Officer uw privacy aanpak in de hele organisatie wil promoten moet u eerst begrijpen wat er precies in de organisatie gebeurt.

In het volgende hoofdstuk van dit handboek worden de eerste stappen gezet naar de ontwikkeling van uw Privacy Aanpak en worden u de bouwstenen aangereikt van het DRAGONFLY Privacy Raamwerk. Een privacy aanpak die altijd begint met het begrijpen van uw organisatie, en dan met name welke persoonsgegevens er worden verwerkt, met welk doel en waar deze worden opgeslagen en bewaard.

3. Wat is een succesvolle Privacy Aanpak?

3.1 Inleiding: het Privacy Raamwerk

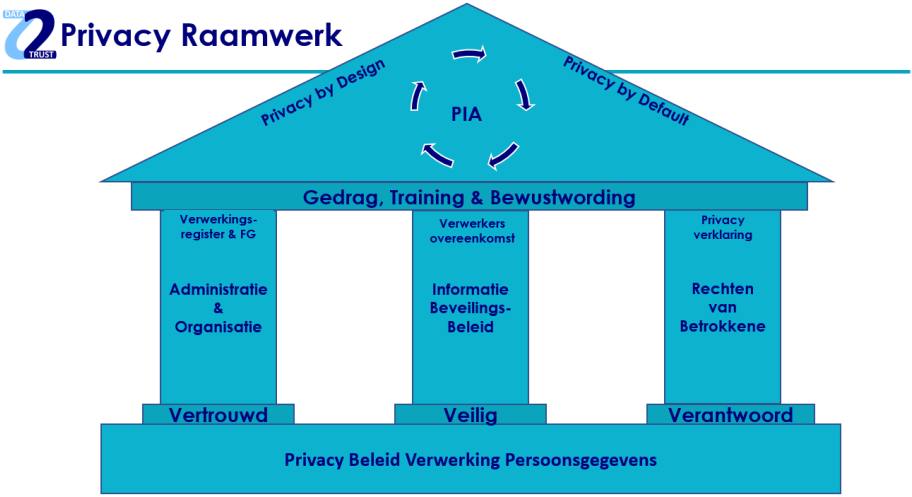
Vanaf 25 mei 2018 moet een organisatie over processen, procedures en systemen beschikken om de naleving van de AVG te waarborgen én u in staat stellen om te gaan met rechten van de betrokkenen zoals uw collega's, klanten en diverse andere stakeholders.

Met andere woorden, de wet vereist dat u over een raamwerk (lees: Privacy-beleid) beschikt waarin:

- Het Verwerkingsregister Persoonsgegevens, de privacy organisatie en het incident management (datalek) is beschreven;
- Het informatiebeveiligingsbeleid in de brede zin – d.w.z. fysiek, organisatorisch en technisch - is uitgewerkt én
- De wijze waarop de verantwoording aan de betrokkenen wordt geregeld.

D2T heeft de wetgeving vertaald naar een overzichtelijk Privacy raamwerk die de AVG vereenvoudigt en de terugbrengt tot de kern: de zogenaamde 3-V's: Vertrouwen, Veiligheid en Verantwoording.

Het raamwerk past op elke organisatie, van groot tot klein, nationaal en internationaal.



Om het raamwerk te bouwen heeft elke organisatie – afhankelijk waar zij staat met haar beveiligingsbeleid - tussen de 5 en 9 documenten nodig om een vliegende start te maken met het 'AVG-compliant' worden. Het opzetten van een Privacy Beleid Verwerking Persoonsgegevens en een Verwerkingsregister Persoonsgegevens zijn de eerste stappen.

Als het fundament en de pijlers stevig genoeg zijn kan gestart worden met de verbinding (bewustwording) en het dak (PIA-cyclus en Privacy by Design). Onderstaand worden per onderdeel de belangrijkste documenten behandeld.

3.2 Fundament: het Privacy beleid

3.2.1 Beleid Verwerking Persoonsgegevens

Met het document '***Beleid Verwerking Persoonsgegevens'*** (inclusief het ***'Datalek protocol'***) zet de organisatie het fundament neer voor Privacybescherming. Dit beleid is de specifieke uitwerking voor de organisatie van de AVG-wetgeving, vertaald naar de drie pijlers: Vertrouwen, Veiligheid en Verantwoording. Gedrag, training en bewustwording is van levensbelang en deze elementen verbinden de drie V's, zodat deze tot het DNA van uw organisatie gaan behoren.

Als sluitstuk zal door wijzigingen in de wetgeving en door technologische ontwikkelingen het raamwerk door de jaren heen veranderen. Om goed in te spelen op deze veranderingen wordt het Privacy-Raamwerk beschermd door de zogenaamde (D)PIA-cyclus (Data Protection Impact Assessment, ook wel gegevensbeschermingseffectbeoordeling genoemd): een gedegen risk assessment als bescherming én als basis voor het vitaal houden van het raamwerk.

3.2.2 Het Datalek-protocol

Vanaf 1 januari 2016 is een data-lek protocol of het melden van datalekken bij de toezichthouder voor iedere organisatie verplicht. Er is sprake van een datalek als persoonsgegevens in handen (kunnen) vallen van derden die eigenlijk geen toegang tot die gegevens zouden mogen hebben. Aanleiding voor een datalek is het constateren van een 'beveiligingsincident'.

Onder de AVG is het van belang dat er een protocol wordt opgesteld waarin het volgende is geregeld:

a) Een centrale registratie van alle datalekken en incidenten;
b) Een duidelijk rapportagemechanisme en escalatieniveau;
c) De verantwoordelijkheid voor de melding, afhandeling en beheer is belegd;
d) Heldere instructie en training voor de medewerkers.

Let op: niet alle incidenten zijn gelijk beveiligingsincidenten. Een passend protocol en instructie ondersteunt de organisatie bij de detectie.

Het beheer van datalekken, incidenten en privacy klachten moet nauwkeurig en grondig worden gedocumenteerd, zodat passende herstelmaatregelen kunnen worden genomen en voor interne en externe auditing-doeleinden.

3.3 Pijler 1: Vertrouwen

Om het vertrouwen te verdienen is het van belang dat de organisatie kan aantonen dat de verwerking van Persoonsgegevens voldoet aan de nieuwe eisen. Kortom: er moet een administratie worden ingericht conform de (administratieve) eisen van de AVG: *het verwerkingsregister Persoonsgegevens*. En mocht er onverhoopt iets fout gaan dan moet de organisatie de beveiligingsincidenten registreren en melden (zie boven: *datalek protocol*).

Tevens moet worden vastgesteld hoe de nieuwe Privacy-taken (zoals het bijhouden van het register) & -rollen belegd worden en hoe deze worden ingebed in de besturing. Kortom: de AVG stelt eisen aan uw organisatie. Daar komen de volgende vragen bij naar voren: Is een Functionaris Gegevensbescherming (FG) verplicht? Kan de borging op een andere wijze worden georganiseerd, bijvoorbeeld door het aanstellen van een Privacy Officer? Hoe wordt de directie betrokken en wat is de rol van het management?

3.3.1 Het Verwerkingsregister Persoonsgegevens

Voor elke dataset (en indien nodig elk gegevenselement) moet de aard van de informatie worden beschreven, welke privacy principes van toepassing zijn en het primaire doel waarvoor de persoonlijke informatie wordt verzameld, gebruikt en openbaar gemaakt.
Dit is het Verwerkingsregister Persoonsgegevens die binnen de organisatie, of onder de verantwoordelijkheid van de organisatie, verwerkt worden. Het register documenteert voor elke dataset de (juridische) onderbouwing van de verwerking. Kort gezegd u documenteert het volgende voor alle belangrijke operationele gebieden van de organisatie:

- Omschrijving welke persoonsgegevens worden verwerkt en wat de rechtsgrond is van de verwerking;
- Waar de persoonsgegevens worden verwerkt in de organisatie, wie de leiding heeft over of verantwoordelijk is voor deze dataset;
- Stel vast of persoonsgegevens bijzondere gegevens bevatten zoals 'gezondheidsinformatie' of andere vormen van 'gevoelige informatie' bevat, waarvoor speciale beperkingen gelden
- Stel vast waarom de informatie wordt verzameld en de doeleinden waarvoor deze worden gebruikt en bekendgemaakt, de bewaartermijn en
- Welke applicatie of IT-systeem wordt gebruikt en welke veiligheidsmaatregelen er zijn getroffen om de gegevens te beschermen;
- Stel vast of informatie namens uw organisatie wordt gehouden door derden, onder meer door IT-leveranciers en dienstverleners, en leg vast waar die derden de gegevens bewaren (waar staan de servers?).

3.3.2 De Functionaris Gegevensbescherming

Vanuit de AVG is het van belang dat (indien van toepassing) de relevante zaken worden gemonitord, beheerd en onderhouden door een functionaris die voor deze taak is toegerust: de Functionaris Gegevensbescherming (FG) of een Privacy Officer. Iedere organisatie is uniek en uitdien hoofde is het van belang om vast te stellen of een FG al dan niet verplicht is.

Er zijn criteria opgesteld om vast te stellen of een FG verplicht is. De benoeming van een FG is verplicht indien:

1. Verwerking wordt uitgevoerd door een publieke autoriteit; of
2. De kernactiviteiten van een verwerkingsverantwoordelijke óf vereist a) "reguliere en systematische monitoring van datasubjecten" óf b) "verwerkingen op grote schaal," of
3. Bestaat uit het verwerken van speciale categorieën van gegevens of gegevens over criminele veroordelingen "op grote schaal."

3.4 Pijler 2: Veiligheid

Hier gaat het om de maatregelen die uw organisatie heeft genomen om de verwerking van Persoonsgegevens adequaat te beveiligen. Het gaat dan om Veiligheid in de brede zin:

- Fysieke beveiliging zoals afsluitbare kasten, toegangscontrole, CCTV. . etc.;
- IT-technische beveiliging zoals firewalls, malware, autorisatie en authenticatie, intrusion detection systems, encryptie . . .etc.;
- Organisatorische beveiliging zoals Clean desk policy, governance; procedures . . .etc.

3.4.1 Het Informatiebeveiligingsbeleid

Informatiebeveiligingsbeleid gaat over meer dan ICT, computers en automatisering. Het gaat om allerlei vormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CCTV, DVD, beeldscherm … etc.) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral mensen en processen.
Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral door menselijk handelen en een tekortschietende organisatie. Ter illustratie de volgende voorbeelden van informatiebeveiligingsmaatregelen: clean desk policy, hoe om te gaan met mobiele devices, screensaver en aanwijzingen voor telewerken.

In de praktijk is de informatiebeveiliging van oudsher sterk gereguleerd bij de massale gegevensverwerkers zoals de (de)centrale overheid, ZBO's, zorginstellingen, verzekeringsmaatschappijen …etc. Er bestaan diverse normeringen en certificeringen om de kwaliteit van de Informatiebeveiliging te borgen, bijvoorbeeld vanuit ISO 27001/27002 en NEN 7510 of de zogenaamde BIG-registers. Het mag duidelijk zijn dat deze een solide basis vormen voor dit onderdeel/ deze pijler binnen het raamwerk. Voert uw organisatie werkzaamheden uit voor dergelijke organisatie waar verwerking van persoonsgegevens mee gemoeid is dan is het niet ondenkbeeldig dat uw beveiligingsniveau als gevolg van de AVG omhoog moet.

Om te komen tot een afgemeten risicobeoordeling van uw beveiligingsbeleid is het aan te bevelen om een IT-kwetsbaarheden onderzoek (Vulnerability scan) uit te voeren. Uit recent onderzoek blijkt dat gebruikte beveiligingssoftware vaak niet up-to-date is en de structurele monitoring van de IT-omgeving daardoor te wensen laat. Met andere woorden: ongewild en ongemerkt blijken er veel 'achterdeurtjes' open te staan.

3.4.2 Verwerkersovereenkomst derden

Uit een onderzoek in 2017 naar de kosten van datalekken bleek dat betrokkenheid van derden-verwerkers de belangrijkste factor was die leidde tot een stijging van (de kosten van) datalekken[5].

Dus als persoonlijke informatie namens u wordt verzameld, opgeslagen of gebruikt door een derde partij, moet het beheer van de privacy risico's een belangrijk onderdeel van uw Privacy Aanpak zijn.
Wanneer uw organisatie de gegevensverwerking (geheel/gedeeltelijk) uitbesteedt aan externe verwerkers, zoals ICT-leveranciers of een salarisadministrateur dan is het belangrijk dat de gemaakte afspraken en bijbehorende contracten die zijn afgesloten voldoen aan de AVG en daarmee a) voldoet aan het veiligheidsniveau (lees: technische en organisatorische maatregelen) van uw organisatie, b) een adequaat datalekprotocol heeft en c) dat medewerkers voldoende zijn opgeleid.

Dit geldt niet alleen voor grote contractpartijen maar ook voor de kleine partijen en ZZP'ers die u heeft ingehuurd en toegang hebben tot persoonsgegevens die u verwerkt. De bestaande contractafspraken en Service Level Agreements (SLA's) moeten aangescherpt met een AVG-bepaling óf er worden separate verwerkersovereenkomsten opgesteld.

3.5 Pijler 3: Verantwoording

Is uw organisatie voldoende flexibel en voldoende transparant om de betrokkene tijdig – binnen de gestelde termijnen – te voorzien van een passend antwoord? Naast administratie, organisatie en een goede beveiliging eist de AVG dat de organisatie lenigheid toont in het bieden van openheid en transparantie rondom de verwerking van Persoonsgegevens.

3.5.1 Protocol Recht van Betrokkene

Recht van betrokkene grijpt in op de klantprocessen van organisaties en ligt derhalve dicht aan tegen klantcontact en een klachtenprotocol.

Onder de AVG heeft de betrokkene recht op inzage, recht op verbetering en aanvulling en recht op afscherming of verwijdering. Voor de afhandeling van verzoeken van betrokkenen gelden wettelijke termijnen (afhandeling inzageverzoek: binnen 4 weken).

Daarnaast moet transparantie en toestemming georganiseerd worden m.b.t. de relatie- of klantdatabase en is het van belang dat de overdracht van persoonsgegevens in een machine leesbaar formaat wordt/is ingeregeld.

Uw organisatie zal procedures nodig hebben voor het behandelen van privacy klachten, die aan alle personeelsleden moeten worden meegedeeld, waaronder:

- Het verschil tussen een privacy klacht en een inzage- of correctieverzoek;
- Wat te doen als een privacy klacht wordt ontvangen;
- Wie moet intern contact opnemen?

[5] Zie https://www.ibm.com/security/data-breach/

- Hoe de klacht vertrouwelijk te houden en persoonlijke gegevens te beschermen;
- Waar om klachten en relevante documenten op te slaan;
- Wie is verantwoordelijk voor het onderzoeken van de klacht;
- Wanneer reageren en hoe;
- Hoe de klacht te onderzoeken;
- Hoe een verslag van het onderzoek te schrijven, en;
- Welke rechtsmiddelen kunnen de klager ter beschikking staan?

3.5.2 De Privacy Verklaring

Een privacyverklaring is een document waarmee de organisatie aan de betrokkene uitlegt welke persoonsgegevens ze verzamelt, wat ze met die gegevens doet en hoe ze deze beveiligt. De specifieke inhoud van de privacyverklaring hangt samen met welk type persoonsgegevens de organisatie verzamelt en hoe ze deze verwerkt. Bepaalde gegevens zijn nu eenmaal gevoeliger dan andere, waardoor de organisatie ook strengere waarborgen moet inbouwen.

Voor alle duidelijkheid privacy beleid moet niet worden verward met de privacy statement.
De Privacy statement is een kennisgeving en zegt iets over de persoonsgegevens en cookies die u verzamelt als uw website wordt gebruikt. Het is een public-facing document en moet gemakkelijk bereikbaar zijn via een link in de voettekst op elke pagina van uw website.

Het is niet de bedoeling dat in Privacy Statements om toestemming wordt gevraagd voor het privacy beleid of voor het verwerken van Persoonsgegevens. De privacy statement is een kennisgeving, niets meer en niets minder. Als het gaat om toestemming dan moeten separaat documenten worden opgebouwd zoals bijvoorbeeld Beleid Verwerking Persoonsgegevens of meer specifiek via zogenaamde Toestemmingsformulieren.

3.6 De verbinding: Training, gedrag & bewustwording

In 2017 is een enquête uitgevoerd onder Privacy Officers en hen een open vraag gesteld: 'Wat zie jij als de grootste uitdaging voor je organisatie?' We verwachtten te horen over sexy onderwerpen zoals Big Data, Anonimisering en Artificial Intelligence, maar in plaats daarvan kwam de meerderheid van de antwoorden neer op één ding: Bewustwording!

Training

Het trainings- of awareness programma ondersteunt naast het verhogen van het beveiligingsbewustzijn de volgende doelstellingen:

- **Kennis**:
  - Medewerkers op de hoogte brengen van het onderwerp privacy in het algemeen;
  - Medewerkers op de hoogte brengen van het onderwerp privacy binnen hun specifieke bedrijf/ organisatie (inclusief de regels voor privacy) in het bijzonder.

- **Houding**:
    - Medewerkers zien het belang en de waarde van informatie voor de organisatie in. Medewerkers zien in dat privacy onderdeel is van hun dagelijkse werkzaamheden.
- **Gedrag**:
    - Medewerkers zetten zich in voor de verbetering van de privacy.
    - Medewerkers spreken elkaar aan op hun gedrag m.b.t. privacy.
    - Medewerkers dragen eigen ideeën aan tot verbetering van de privacy.

Om deze doelstellingen te behalen en de gewenste bewustwording te realiseren is het essentieel om deze in fasen te doorlopen. Om ervoor te zorgen dat de medewerkers van de organisatie alle fasen doorlopen, wordt een communicatieplan opgesteld. Hierbij is het van belang dat de communicatie over privacy gedurende alle fasen herkenbaar is.

3.6.2 Gedrag: Tone-at-the-Top

De cultuur van een organisatie - weerspiegeld in het gedrag en overtuigingen van personeel en management - bepaalt hoe de dingen worden gedaan. Tone-at-the-top oftewel eigenaarschap van het topmanagement en voorbeeldgedrag zijn essentieel voor het bevorderen van een Privacy-cultuur in een organisatie.

Het senior management kan uw Privacy aanpak actief ondersteunen door:

- Aanwijzen van een sponsor in het (senior) management of directieteam
- Formeel de aanpak goed te keuren;
- Voldoende middelen beschikbaar te stellen voor de uitvoering van het programma;
- Regelmatig te rapporteren over de mijlpalen van het programma, en
- Voorbeeldgedrag: volgen en verdedigen van privacy beleid en procedures (let wel: iets eenvoudigs als clean desk blijkt vaak al een uitdaging . . .).
- Actieve bijdrage aan (D)PIA's, audits en het opvolgen en implementeren van verbetervoorstellen.

Wil het topmanagement u als Privacy Officer en uw team écht als toegevoegde waarde gaan zien dan moet uw rol meer inhouden dan het waarschuwen voor privacy risico's en het verzorgen van trainingsprogramma's voor medewerkers. De top wil weten hoe zij - door het maximale uit hun data te halen - de operationele effectiviteit kan vergroten, zonder dat er reputatieschade of anderszins juridische averij wordt opgelopen.

Uw rol gaat om het stimuleren van een nieuw besef bij het Topmanagement. Namelijk, het besef dat Privacy een nieuwe dimensie toevoegt aan de medewerker tevredenheid en klantgerichtheid van uw organisatie en dat het vertrouwen in uw Privacy aanpak eerder een 'business' driver is dan een beperking!

3.6.3 Bewustwordingsprogramma

Een bewustwordingsprogramma is een integraal onderdeel van het Privacy beleid. Een goed opgezet bewustwordingsprogramma voorziet in een reeks primaire stappen om de interne bewustwording te laten ontstaan en te vergroten.

Bewustwording betekent het bewust zijn van risico's die er bestaan op het gebied van privacy. Bepaalde risico's kunnen worden beperkt door het treffen van technische

maatregelen. Maar veel risico's liggen in het handelen als onderdeel van menselijk gedrag. Het bewustwordingsprogramma richt zich daarom vooral op het aspect menselijk gedrag.

Centrale vraag:
Hoe maak je medewerkers duidelijk, dat hun eigen gedrag voor een groot deel bepalend is voor de mate waarin risico's worden gelopen op het gebied van privacy?

3.7 Het Dak: (D)PIA en Privacy by design

Een veel gehoorde term als het gaat om de AVG is de Privacy Impact Assessment, afgekort de PIA. In Nederland spreekt men van Gegevensbeschermingseffectbeoordeling (GEB). Een leuk scrabble-woord, ofschoon je met alleen de 'e' al aardig op weg bent. De AVG stelt een impact assessment in bepaalde gevallen verplicht[6]. Dat is in ieder geval zoals een organisatie:

1. Systematisch en uitvoerig persoonlijke aspecten evalueert, waaronder profiling;
2. Op grote schaal bijzondere persoonsgegevens verwerkt;
3. Op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht);

Om te bepalen of er mogelijk sprake is van een hoog risico hanteren de toezichthouders de onderstaande vuistregel. Er is sprake van een hoog risico als men aan twee of meer van de onderstaande negen criteria voldoet:

a) Evaluatie van personen of scoretoekenning;
b) Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg;
c) Stelselmatige monitoring;
d) Gevoelige gegevens of gegevens van zeer persoonlijke aard;
e) Op grote schaal verwerkte gegevens;
f) Matching of samenvoeging van datasets;
g) Gegevens met betrekking tot kwetsbare betrokkenen;
h) Innovatieve toepassing van nieuwe technologische of organisatorische oplossing;
i) Blokkering van een recht, dienst of contract.

Wat deze PIA precies inhoudt is niet altijd even bekend bij organisaties en het voldoen aan deze eis wordt dan lastig. Daarbij zijn er verschillende soorten PIA's in omloop en ook de tooling om hierbij te ondersteunen wordt steeds meer aangeboden.

3.7.1 Handreiking PIA

Voor voorstellen/ projecten waarbij het verzamelen, gebruiken of openbaar maken van persoonlijke informatie op nieuwe manieren plaatsvindt, moet u een Privacy Impact Assessment (PIA) uitvoeren of laten uitvoeren, of op zijn minst enige vorm van Privacy-

[6] In geval van een verplichting spreekt men van een DPIA oftewel Data Protection Impact Assessment

risicobeoordeling van het voorstel/ project. De PIA is dan niets meer en niets minder dan risico gestuurde Privacy assessment.

De belangrijkste uitdagingen zijn:

- Inbedden van de Privacy risicobeoordeling in de reguliere projectbesturing – zowel bij de initiatie als het beheer van een project - binnen de organisatie;
- Beoordelen wanneer een minimale risicobeoordeling nodig is – de zogenaamde pre-PIA afgezet tegen de uitgebreidere PIA, en eventueel de Functionaris Gegevensbescherming om advies vragen;
- Team samenstellen, bepalen wie de PIA moet uitvoeren, wie de PIA faciliteert en wie moet rapporteren, en
- Vaardigheden ontwikkelen om risico's te detecteren, oorzaken en gevolgen te benoemen en maatregelen te formuleren die Privacy risico's verminderen of wegnemen.

Het zijn niet alleen nieuwe projecten of derden die privacy risico's kunnen creëren voor uw organisatie. Soms is het de status-quo - of 'zo doen we dat nu eenmaal' - wat risico's voor u kan opleveren. Een privacy risicobeoordeling van de bestaande Verwerkingspraktijk van de organisatie - beter bekend als een privacy audit of compliance review - moet daarom met regelmatige tussenpozen worden uitgevoerd.

Hoewel audits de status-quo bekijken, terwijl PIA's over het algemeen zijn ontworpen voor nieuwe projecten, is de methodiek voor het identificeren en beperken van privacy risico's vergelijkbaar.

3.7.2 Privacy by design

In de AVG wordt Privacy by Design vereist bij het verwerken van persoonsgegevens. Privacy by Design betekent dat de organisaties bij de ontwikkeling van nieuwe producten en diensten zo vroeg mogelijk aandacht besteden aan het beschermen van persoonsgegevens. Het houdt in dat er al bij de ontwikkeling van producten en diensten aandacht moet zijn voor privacy.

In het bijzonder bij ICT-producten en -diensten gaat het erom dat al in het ontwikkelproces gebruik gemaakt wordt van privacy-verhogende maatregelen (ook wel *privacy enhancing technologies* of PET genoemd).

Verschillende aspecten spelen hierbij een rol. Je kunt je bijvoorbeeld afvragen of het voor het product of de dienst écht nodig is om persoonsgegevens te verwerken (doelbinding) of dat er bijvoorbeeld ook gewerkt kan worden met volledig geanonimiseerde gegevens. Als er dan toch persoonsgegevens verwerkt gaan worden, is het van belang om na te denken over de beveiliging van deze gegevens.

Dat kan bijvoorbeeld door pseudonimiseren (anders dan bij anonimiseren worden de gepseudonimiseerde gegevens nog steeds gezien als persoonsgegevens), door encryptie en met behulp van acces control.

Ook bewaartermijnen of opslagbeperking en het faciliteren van de rechten van de betrokkenen zijn van belang om privacy-proof te opereren. Daarnaast zijn data-minimalisatie en privacy by default onderdelen van Privacy by design. Deze termen lichten we hieronder kort toe.

Data-minimalisatie

Een belangrijk onderdeel van privacy by design is data-minimalisatie. In het ontwerp moet gewaarborgd worden dat er niet méér persoonsgegevens verwerkt worden dan strikt noodzakelijk voor het doel van de verwerking.

Privacy by default

Privacy by default kan gezien worden als een onderdeel van privacy by design. Privacy by default vereist dat de standaardinstellingen vooraf altijd zo privacy-vriendelijk mogelijk ingesteld zijn.

Er moet voor gezorgd worden dat persoonsgegevens nooit standaard openbaar zichtbaar zijn. Het meest sprekende voorbeeld is uw profiel op social media. Dit mag wel openbaar zijn, maar slechts als u daar zélf actief voor kiest. De social media-toepassing zal in de standaardinstellingen de gebruikersprofielen zoveel mogelijk moeten afschermen.

Dit principe van het afschermen van persoonsgegevens geldt voor alle ICT-toepassingen: van browser-instellingen tot aan de bedrijfs-app.

Vergelijk het met nieuwsbrieven. Tegenwoordig vereist de Telecommunicatiewet dat sprake is van een 'opt-in' voor nieuwsbrieven; je moet je actief voor een nieuwsbrief aanmelden en deze mag dus niet standaard aangevinkt staan. Zo is het ook met privacy: deze moet standaard zo hoog mogelijk zijn en je moet mensen actief laten kiezen voor het breder laten delen van hun gegevens.

4. Hoe nu verder?

4.1 Inleiding

Nu u alles heeft gelezen wat er bij een goede Privacy Aanpak voor uw organisatie komt kijken, is het tijd om even achter over te zitten te reflecteren op uzelf. Om een goede Privacy Officer te zijn moet u de AVG-wetgeving beheersen en bóvenal de vaardigheden ontwikkelen om Privacy risico's te detecteren en op te lossen.

4.2 Beter GRIP op AVG

D2Tis erop gericht organisaties te ontzorgen door middel van het bieden van een solide AVG-raamwerk. Om dit raamwerk te bouwen, te implementeren en te onderhouden biedt DGF drie typen dienstverlening aan, te weten:

Toelichting:
De **AVG Management Tool** is de geautomatiseerde (SAAS) toepassing van het Privacy-raamwerk uit het voorgaande hoofdstuk. Met deze tool brengt u uw basis hygiëne AVG op orde en heeft u GRIP op Privacy. GRIP betekent dat de organisatie tijd kan besteden aan echt ondernemerschap: werken aan new business, marketing & sales, digitalisering, relaties met bestaande klanten verdiepen en natuurlijk aandacht voor uw medewerkers.

Want met de hygiëne op orde kan AVG worden ingezet als ondersteuning van het ondernemerschap en de plannen. Enerzijds door het bieden van een **expert- en adviesfunctie** AVG, Coaching en Begeleiding van Privacy Officers, Begeleiden van Implementatie en Audits tot het bieden van een Functionaris Gegevensbescherming.

Anderzijds is het **getraind en bewust** houden van personeel op Privacyaspecten binnen uw organisatie een belangrijke opdracht. Afhankelijk van het type organisatie en de gevoeligheid van de persoonsgegevens die u verwerkt kan D2T Privacy & Security een passend opleidingsaanbod te doen.

4.3 Consultant Privacy & Security

D2T ziet het als haar primaire taak om organisaties te ondersteunen en te adviseren op weg naar AVG compliancy. D2T beschikt over gecertificeerde Consultants Privacy & Security - die volledig zijn ingevoerd in het D2T-raamwerk en hun kennis breed kunnen inzetten.

De inzet van de D2T-Consultant betekent dat de organisatie enerzijds kiest voor de gestandaardiseerde D2T-aanpak en anderzijds voor maatwerk omdat het raamwerk op maat wordt gemaakt voor de organisatie. Met de inzet van de Consultant bedoelen we het volgende:

- Functionaris Gegevensbescherming & Privacy Officers
- Implementeren van SAAS-toepassingen.
- Implementeren van AVG én E-privacy wetgeving
- Uitvoeren van de classificatie van persoonsgegevens
- Implementeren van AVG beproefde registratiewijzen van persoonsgegevens
- Implementeren van procedures rondom incidentmanagement en datalekken
- Beleid formuleren over privacy, informatiebeveiliging en de verwerking van gegevens
- Advies op snijvlak van privacy, (cyber) security en bedrijfsvoering
- Opzetten en implementeren van verwerkersovereenkomsten
- Opzetten en implementeren van Privacy Statements
- Uitvoeren en begeleiden van DPIA's (risico assessment en GAP-analyse)
- Registratie van D2T FG/DPO bij de Autoriteit Persoonsgegevens
- Uitvoeren en ondersteunen FG-werkzaamheden.

Tenslotte,
D2T is onafhankelijk en werkt nauw samen met een groot aantal leveranciers op het gebied van Privacy software, awareness trainingen, cyber-securityoplossingen …etc. Dit maakt het mogelijk om met de implementatie van het D2T-raamwerk nauw aan te sluiten bij organisatorische en technische infrastructuur van de organisatie en bovendien de kosten acceptabel te houden

Kwalificatie en beperking

Deze publicatie vormt geen juridisch advies en mag niet worden beschouwd als een juridisch advies van een partij.

Over de auteur

Dit handboek is opgesteld door Douwe Cnossen, adviseur en lead consultant Privay & Security.

Douwe is een all-round Privacy & Security Professional (CISSP | CIPM | CTPP), DPO en trusted advisor. Econoom (drs.) met postdoctorale specialisaties als Register Controller op data-governance, risk & control en als MBA op Public Governance.

Douwe heeft ruim 20 jaar ervaring in de Brede Bedrijfsvoering, variërend van Direct Report tot '*die hard*' professional en adviseur.
Ervaring bij grote Verzekeraars in zowel de publieke als de private sector (UWV, Achmea). Via diverse consultancybureaus werkt hij de vanaf 2016 als adviseur en lead consultant in uitlopende sectoren van Multinational tot MKB en geeft trainingen en lezingen in privacy & security awareness. Naast dit handboek schreef hij BLOGS over informatiebeveiliging en privacy.

6. BIJLAGEN

TEMPLATE: Privacy beleid verwerking Persoonsgegevens

TEMPLATE: Datalek protocol

TEMPLATE: Verwerkingsregister Persoonsgegevens

TEMPLATE: Functiebeschrijving FG

TEMPLATE: Samenvatting ISO 27001

TEMPLATE: Verwerkersovereenkomst

TEMPLATE: Informatiebeveiligingsbeleid (ISO 27001 als basis)

TEMPLATE: Protocol recht van betrokkene

TEMPLATE: Privacy Verklaring + Cookie statement

TEMPLATE: Bewustwordingsprogramma

TEMPLATE: Handreiking DPIA

TEMPLATE: Privacy by design

Contact

Heeft u vragen inzake de AVG of de rol van Privacy Officer, neem dan contact op via een van de onderstaande optie's.

info@d2trust.nl

Telefoon. +316 14 94 33