Whitepaper ‘Privacy management en de AVG in vogelvlucht’

Veel organisaties zijn al sinds de inwerkingtreding van de AVG op risico gebaseerde wijze actief aan de slag met de aantoonbare implementatie, naleving en beheersing van de AVG-vereisten. Hiervoor hebben organisaties al veel acties ondernomen. Door deze veelheid aan acties is het wellicht af en toe lastig om het ‘grotere plaatje’ te (blijven) overzien, waardoor niet altijd duidelijk is hoe de individuele acties bijdragen aan het grote geheel van AVG-compliance. Dit whitepaper is bedoeld om hier helderheid in te verschaffen. Ook geeft het een totaaloverzicht van de stappen die al zijn gezet en welke stappen nog noodzakelijk zijn.

1. Privacy management is meer dan alleen AVG-compliance

In de praktijk zien wij vaak dat het waarborgen van de privacy van betrokkenen (p*rivacy management*) gelijk wordt gesteld aan het naleven van de AVG. Dit uit zich in vragen als ‘Mag dit van de AVG?’ of ‘Wat zegt de AVG hierover?’. Echter, het waarborgen van de privacy van betrokkenen gaat om (veel) meer dan alleen het naleven van de AVG (zie Figuur 1).

Figuur 1 – De elementen van Privacy management

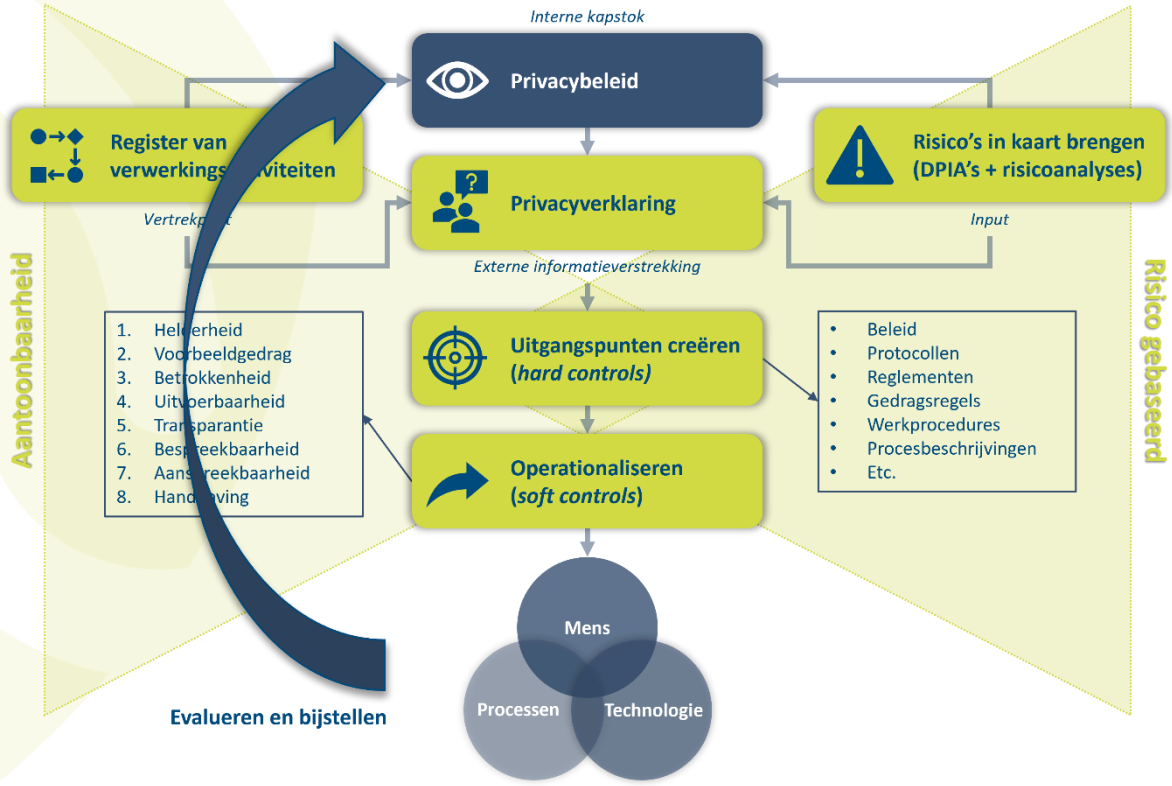
In essentie staat *vertrouwen* centraal bij privacy management. Het gaat hier om het vertrouwen dat betrokkenen (en andere stakeholders) er in hebben dat de organisatie de privacy van betrokkenen waarborgt. De missie, visie en strategie van een organisatie weerspiegelt over het algemeen hoe de organisatie daarmee omgaat. Om vertrouwen te creëren, zijn *legitimiteit*, *verantwoordelijkheid* en

eerlijkheid noodzakelijk. Om dit te bewerkstelligen, moet de organisatie aandacht besteden aan (kortweg) drie elementen, te weten *ethiek*, *compliance* en *transparantie*.

Dit betekent dat de organisatie allereerst de ethische kant van privacy management onder de loep moet nemen: 'Willen we eigenlijk echt wel doen wat wij bedacht hebben?' en 'Mogen we doen wat we willen doen?' Vervolgens is de vraag 'Doen we dat op een verantwoorde manier?' Dit betreft de naleving van de AVG, het compliance-element (hierover meer in de volgende paragraaf). En tot slot moet een organisatie zich de vraag stellen: 'Leggen we duidelijk uit wat we doen?', het transparantie-element.

2. De route naar AVG-compliance

Zoals hiervoor aangegeven, gaat privacy management dus niet alleen over AVG-compliance. Dit is echter wel een essentieel onderdeel van privacy management. Daarom is in dit hoofdstuk de route naar AVG-compliance nog eens kort uiteengezet en hieronder weergegeven (zie Figuur 2).



Figuur 2 – De route naar AVG-compliance in één oogopslag

Privacybeleid als interne kapstok

Aan de start van de route naar AVG-compliance staat het privacy- en informatiebeveiligingsbeleid. Het doel van het beleid is om richting te geven aan de organisatie en hiermee ook de spelregels bepalen. In het beleid geeft een organisatie aan hoe zij aan de AVG voldoet/gaat voldoen. Hierin staan (onder andere) de kernpunten, zoals visie, reikwijdte en raakvlakken met ander beleid in de organisatie. Ook

is hierin de organisatiestructuur (*governance*) opgenomen, zodat de taakverdeling duidelijk is en het eigenaarschap is belegd.

Het toepassen van de regels uit de AVG is niet een *one size fits all* aangelegenheid. Het moet worden toegesneden op de eigen organisatie. Het beleid (en de beheersmaatregelen) worden afgestemd op de processen, verwerkingen van de organisatie en de privacyrisicos voor de betrokkenen. Daarom is het advies om zowel het register van verwerkingsactiviteiten als DPIA's en risicoanalyses als vertrekpunt en input te gebruiken. Ook zijn onze AVG-Zelftoets en FG-rapportages hiervoor goed bruikbaar.

Transparantie over het beleid en uitgangspunten formuleren

Nadat het beleid is vastgesteld, is het van belang om hierover transparant richting betrokkenen te zijn. Ook is het noodzakelijk om inzicht te geven in de verwerking van persoonsgegevens door de organisatie en de mogelijke risico's hiervan. Doorgaans gebeurt dit door het opstellen en publiceren van privacyverklaringen (bijvoorbeeld op de website of het intranet), of door middel van actievere communicatie (bijvoorbeeld specifieke brieven/e-mails of andere berichtgevingen).

Daarnaast is het van belang om uitgangspunten te formuleren die helpen bij het operationaliseren van het beleid en het nemen van beheersmaatregelen, op een risico gebaseerde manier. Dit kan bijvoorbeeld door uit de grote hoeveelheid regels en voorschriften uit de AVG (173 overwegingen en 99 artikelen) de belangrijkste onderwerpen (*controls*) te distilleren en hierop acties uit te zetten en beheersmaatregelen in te richten. Lumen Group heeft, in navolging van de AP, datzelfde gedaan door de AVG-vereisten terug te brengen naar de 10 belangrijkste onderwerpen (zie hoofdstuk 2).

Aandacht verdient ook het *aantoonbaar* naleven van de regels uit de AVG, een heel belangrijk onderdeel van deze wet. Dit kan door het opstellen van gericht beleid en uitwerking in protocollen, reglementen, gedragsregels, werkprocedures en procesbeschrijvingen. Voorbeelden hiervan zijn een protocol voor de afhandelingen van datalekken en incidenten en een beleid voor het bewaren en vernietigen van de persoonsgegevens.

Operationaliseren van het beleid en nemen van beheersmaatregelen

Nadat de uitgangspunten van het beleid verder zijn bepaald en uitgewerkt, is het van belang om het beleid daadwerkelijk te operationaliseren. Over het algemeen wordt het aangeraden om hiervoor op drie vlakken beheersmaatregelen te nemen, te weten: *processen*, *technologie* en de *mens*.

Op het gebied van *processen* geldt dat dit kan door bijvoorbeeld het in lijn brengen van processen/werkwijzen met het beleid, het zorgen voor een goed incidentmanagement (bijvoorbeeld door het adequaat afhandelen van datalekken en beveiligingsincidenten) en het inrichten van toezicht en controle (bijvoorbeeld door het controleren van de logging en hier ook op sturen). Ten aanzien van de *technologie* kan gedacht worden aan het technisch afdwingen van bepaalde maatregelen

(bijvoorbeeld het in systemen instellen van bewaartermijnen), het gebruik van sterke authenticatie-methoden, het beheren van autorisaties en het versleutelen (encryptie) van persoonsgegevens.

Meestal is de *mens* de zwakste schakel in de gehele keten. Daarom moet hier extra aandacht aan besteed worden. Uit de 'Rapportage datalekken 2020' van de AP blijkt namelijk dat 84% van de datalekken in 2020 is ontstaan door menselijk handelen. Het stimuleren van privacybewust gedrag en cyberhygiëne onder medewerkers is van het grootste belang. Besteed daarom structureel aandacht aan bewustwording, het bijbrengen van kennis en het trainen van medewerkers over hoe te handelen in specifieke situaties.

Evalueren en bijstellen als onderdeel van de PDCA-cyclus

Nadat het beleid (volledig) is geoperationaliseerd en de beheersmaatregelen zijn genomen, is de volgende stap om – als onderdeel van de PDCA-cyclus – het beleid en de genomen beheersmaatregelen periodiek te evalueren en, indien nodig, bij te stellen. Een PDCA-cyclus borgt periodieke controles, toetsing en evaluaties en eventueel aanpassingen. Kernonderdelen van de cyclus zijn inzicht in de stand van zaken, checks op tijd, kwaliteit en werking, betrokkenheid en (bij)sturing op diverse (bestuurs)niveaus binnen de organisatie, verantwoording en transparantie.

Raadpleeg de 'Handreiking PDCA-cyclus voor privacy en informatiebeveiliging', inclusief handige voorbeeldstuurvragen en een voorbeeld van een AVG-checkplan van Lumen Group, voor meer ondersteuning hierbij.

3. FG-dienstverlening Lumen Group

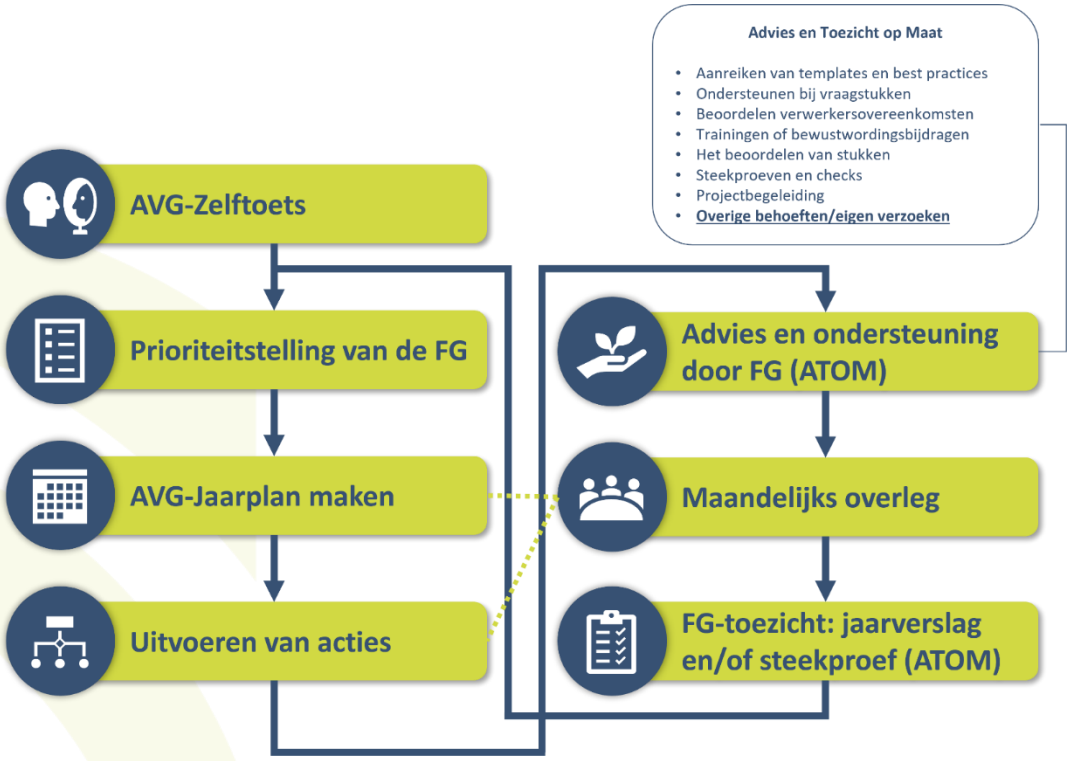
Binnen het FG-abonnement dat klanten met Lumen Group hebben afgesloten, ondersteunt en adviseert Lumen Group de klant richting AVG-compliance. In dit hoofdstuk hebben wij in een notendop nog weergegeven wat de FG-dienstverlening van Lumen Group inhoudt. In veel gevallen hebben wij aanvullingen gedaan op de diensten die Lumen Group reeds binnen het FG-abonnement leverde, zodat wij van toegevoegde waarde voor klanten blijven.

Advies en toezicht op maat (ATOM) als centrale pijler

Wij geven onze FG-dienstverlening vorm aan de hand van onze *Advies en toezicht op maat (ATOM)* aanpak. Hierbij kunnen organisaties, naast de verplichte FG-dienstverlening, en in samenspraak met Lumen Group, deels *zelf een advies- en toezichtspakket samenstellen*. Zo kunnen organisaties kiezen uit onder andere het geven van (bewustwordings)training en doelgerichte sturing en prioriteitstelling voor de implementatie van de AVG.

FG-aanpak en -roadmap

Hieronder is onze FG-aanpak en -roadmap weergegeven (zie Figuur 3). Deze wordt stapsgewijs toegelicht.



Figuur 3 – FG-aanpak en -roadmap

Doorgaans vangt onze FG-dienstverlening aan met een *AVG-Zelftoets*. In samenspraak kan er echter ook voor worden gekozen om direct een *AVG-Steekproef* te verrichten. Op basis van de uitkomsten is er een *prioriteitstelling* opgesteld, welke organisaties daarna vertalen naar een *AVG-Jaarplan*. Vervolgens wordt er uitvoering gegeven aan het AVG-Jaarplan en worden er concrete *acties uitgevoerd*.

Lumen Group ondersteunt en adviseert organisaties bij het uitvoeren van deze acties door middel van aanreiking van passende en beproefde *AVG-templates* en *andere hulpmiddelen, de Lumen Toolbox*, waarover verderop meer. Dat gebeurt ook door de *beschikbaarheid van het Lumen Group Team* voor de eigen Privacy Coördinator voor o.a. eerstelijnsvragen die gerelateerd zijn aan de AVG/privacy en de FG (toezichts)functie. Tevens ondersteunt Lumen Group door het *beoordelen van documenten* (zoals beleidsstukken en verwerkersovereenkomsten) en het *geven van trainingen* of het geven van *bewustwordingstrainingen* of bijdragen aan *bewustwordingsactiviteiten*.

Verder heeft Lumen Group met de Privacy Coördinator van organisaties *maandelijks een digitaal overlegmoment* om de interne stand van zaken rondom de AVG te bespreken en om de laatste belangrijke ontwikkelingen te delen. Tijdens deze overlegmomenten ondersteunt Lumen Group bij bestaande AVG-uitdagingen door best practices, templates en pragmatische adviezen te suggereren.

Tot slot houdt Lumen Group *risico-gebaseerd toezicht* op naleving van de AVG als 'critical friend', toegespitst op de organisatie. Hierbij geven wij onder andere *pragmatische gevraagde en ongevraagde*

adviezen. Ook het uitvoeren van *AVG-Steekproeven*, het opstellen van *onafhankelijke (jaar)rapportages* met bevindingen en aanbevelingen en het *beoordelen van documenten en werkwijzen* hoort daarbij.

Lumen Toolbox

Onderdeel van het FG-abonnement zijn passende en beproefde AVG-templates en andere hulpmiddelen die Lumen Group heeft ontwikkeld. Hieronder is weergegeven wat binnen onze Lumen Toolbox valt (zie Figuur 4).

Figuur 4 – Lumen Toolbox