1. Toelichting Lumen Group Privacyvolwassenheidsmodel

De steekproef wordt verricht op basis van het Lumen Group Privacyvolwassenheidsmodel. In dit model staan privacyvolwassenheidsniveaus centraal. Het model bevat individuele toetsingskaders met betrekking tot privacy- en informatiebeveiligingsonderwerpen.

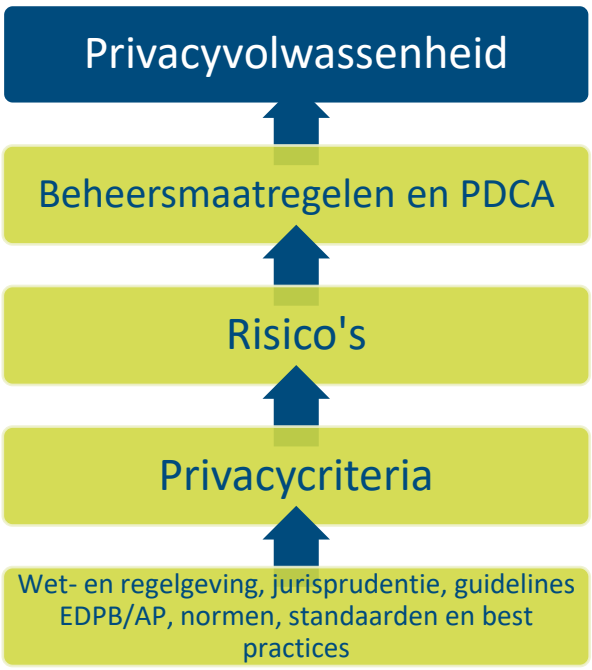
Doel en uitgangspunten

Het Lumen Group Privacyvolwassenheidsmodel biedt organisaties handvatten om privacyrisico's structureel inzichtelijk te maken, zodat deze risico's beheersbaar kunnen worden gemaakt door de organisatie. Daardoor is er sprake van een risico-gebaseerde aanpak die privacywet- en regelgeving van organisaties vereist.

Doordat het model bestaat uit specifieke toetsingskaders die zijn onderverdeeld in verschillende (volwassenheids)niveaus, kan de daadwerkelijke situatie van de implementatie van privacywet- en regelgeving worden vergeleken met het streef- en/of ambitieniveau van een organisatie. Een bijkomstigheid daarbij is dat een vorm van herkenbaarheid wordt verschaft. Door het vertalen van risico's naar concrete beheersmaatregelen is er sprake van herkenbaarheid aan de zijde van de organisatie. Daardoor sluiten de oplossingen aan bij de organisatieprocessen, wat maakt dat het voor organisaties makkelijker is om risico's te beheersen.

Toepassing en verantwoording

De individuele toetsingskaders bevatten normen die voortvloeien uit wet- en regelgeving (zoals o.a. AVG, UAVG en EVRM), jurisprudentie, richtlijnen van de EDPB/AP, normen, standaarden (zoals o.a. ISO270001/270002) en best practices. Al deze normen zijn voor elk individueel toetsingskader vertaald naar specifieke (privacy)criteria. Tevens is kwaliteitsmanagement (door bijvoorbeeld de PDCA-methodiek) onderdeel van de toetsingskaders. Deze structuur maakt dat de kwaliteit van de inhoudelijke en organisatorische implementatie van de privacywet- en regelgeving gewaarborgd, gecontinueerd en, waar mogelijk, kan worden verbeterd.



Het Lumen Group Privacyvolwassenheidsmodel is gebaseerd op de *Capability Maturity Model Integration* (afgekort CMMI). De CMM(I)-methodiek is een gerespecteerde methode en wordt in diverse sectoren gebruikt. Zo wordt de methode onder andere, op voorschrijven van de Koninklijke

Nederlandse Beroepsorganisatie van Accounts, gebruikt door accountants in de branche van informatiebeveiliging. Daarnaast wordt de methode ook gebruikt door het Centrum Informatiebeveiliging en Privacybescherming (CIP).

Meer weten over onze onderliggende beoordelingsmethode met de privacyvolwassenheidsniveaus en verantwoording daarvan? Neem dan gerust contact met ons op. Wij lichten dit graag verder toe.

2. Algemene beschrijving privacyvolwassenheidsniveaus

Binnen het Lumen Group Privacyvolwassenheidsmodel worden vijf niveaus gehanteerd (1 t/m. 5). Hieronder volgt een algemene beschrijving van de kerncriteria van elk privacyvolwassenheidsniveau.

1. Ad hoc	2. Herhaalbaar	3. Vastgesteld	4. Beheerst en meetbaar	5. Geoptimali-seerd
Ad hoc keuzes vanuit persoonlijk perspectief	Het beleid is opgezet	Het beleid is bestaand	Het beleid is werkend	Gehele organisatie kan externe factoren en ontwikkelingen anticiperen en haar strategie aanpassen
Keuzes op in concrete gevallen en op verwerkingsniveau	Keuzes niet meer op verwerkingsniveau	Keuzes op basis van operationeel beleid, richtlijnen en werkinstructies op organisatieniveau	Sturing van verwerkingsactiviteiten op snelheid, kwaliteit en interactie op basis van de PDCA-cyclus	Mogelijk om voorafgaande prognoses over kosten en reactiesnelheid, die leiden tot weloverwogen beslissingen en effectieve, adequate uitkomsten
Wel sprake van vastlegging, geen sprake van vaststelling	Keuzes op basis van beleid, richtlijnen en werkinstructies op afdelingsniveau	Operationeel beleid, richtlijnen en werkinstructies vastgesteld op organisatieniveau en formele bekrachtigd	Operationele werkelijkheid wordt door middel van de PDCA-cyclus bewaakt	Operationele werkelijkheid kan worden aangepast om beleidsdoelen na te streven;
Geen sprake van beleid	Structurele rapportage op afdelingsniveau over de bescherming van persoonsgegevens	Structurele rapportage is nog niet ingericht	Volledige transparantie richting stakeholders, welke zichtbaar en meetbaar is voor de hele organisatie	Beleidsmatige niveau kan huidige stand van zaken inzien en vergelijken met de branche;
	Geen formeel vastgesteld beleid op organisatieniveau	Sturing in overleg met bestuur op organisatieniveau	Het bestuur is betrokken bij controle en informatie	

3. Beoordelingsraamwerk AVG-Steekproef

Onderwerp	Privacycriterium	Privacyrisico('s)
1 ***Privacybeleid en governance***	Een verwerkingsverantwoordelijke is verplicht privacybeleid te hebben en in dat kader maatregelen toe te passen om te voldoen aan (privacy)wet- en regelgeving, en in sommige gevallen ook aan contractuele bepalingen. Het is vereist dat de organisatie rekening houdt met de aard, omvang, context en het doel van de verwerkingen binnen de organisatie. Het is de verplichting van de verwerkingsverantwoordelijke om te waarborgen én aan te tonen dat zij persoonsgegevens verwerkt in overeenstemming met de AVG. Voor organisaties bestaat de kans dat men zich uitsluitend richt op het beschermen van persoonsgegevens van externe stakeholders (bijv. klanten, leden, leerlingen of patiënten). Echter, een organisatie moet zich ook richten op de bescherming van persoonsgegevens van interne stakeholders (bijv. werknemers en opdrachtnemers). In dat kader is het een organisatie dus verplicht een privacybeleid te voeren en te hanteren dat (ook) de bescherming van de persoonsgegevens van interne stakeholders betreft.	Het vastleggen en hanteren van beleid is een vorm van zelfbinding en kwaliteitswaarborging. Indien een verwerkingsverantwoordelijke geen privacybeleid vastlegt en hanteert, dan kan zij niet (op afdoende wijze) de privacy van betrokkenen waarborgen. Daarnaast kan men zich niet aantoonbaar verantwoorden. Als binnen de organisatie niet is beschreven op welke wijze de organisatie omgaat met de privacy van betrokken, kan als gevolg daarvan de kwaliteit van de dienstverlening/het product van de organisatie niet (afdoende) worden gewaarborgd. Ook bestaat het risico dat in het geval van incidenten, de organisatie niet op adequate wijze weet te handelen omdat het simpelweg geen beleid heeft om de incidenten te beheersen. Een algemeen risico is dat de organisatie reputatieschade oploopt en dat Autoriteit Persoonsgegevens (hoge) boetes kan opleggen. Organisaties hebben de neiging om beheersmaatregelen te nemen die gericht zijn op de bescherming van de privacy van externe stakeholders (bijv. klanten, leden, leerlingen of patiënten). Bij afwezigheid van beheersmaatregelen die (eveneens)

			op interne stakeholders (bijv. werknemers en opdrachtnemers) zijn gericht, loopt de organisatie het risico dat zij daardoor de rechten van deze betrokkenen schaadt als er iets mis gaat en daarmee de wet overtreedt. Hierdoor bestaat er een risico op reputatieschade en een (hoge) boete, op te leggen door de Autoriteit Persoonsgegevens.
2	***Informatieplicht (privacyverklaring)***	De organisatie informeert interne en externe betrokkenen van wie persoonsgegevens worden verwerkt op beknopte, transparante, eenvoudig toegankelijke wijze, en in begrijpelijke, duidelijke en eenvoudig taal, over het privacybeleid van de organisatie.	De AVG kent een expliciete informatieplicht voor organisaties die persoonsgegevens verwerken. Als een organisatie haar betrokkenen niet informeert over de wijze waarop zij met de persoonsgegevens en privacy van haar betrokkenen omgaat, is zij onvoldoende transparant en weten de betrokkenen niet waar zij aan toe zijn. Dit geldt als een directe schending van wet- en regelgeving en kan leiden tot reputatieschade voor de organisatie en een (hoge) boete, op te leggen door de Autoriteit Persoonsgegevens.
3	***Register van verwerkingsactiviteiten***	De verwerkingsverantwoordelijke (en verwerker) houden een register bij waarin hun verwerkingsactiviteiten zijn opgenomen (verwerkingsregister of dataregister). Dit register biedt een actueel, volledig en samenhangend overzicht van de gegevensverwerkingen.	Indien een verwerkingsverantwoordelijke geen register met daarin haar verwerkingsverantwoordelijkheden opstelt, dan heeft zij geen inzicht in welke persoonsgegevens en op welke wijze de organisatie persoonsgegevens van betrokkenen verwerkt. Door de afwezigheid of incompleetheid van het verwerkingsregister is het niet mogelijk voor een organisatie om privacyrisico's

			(volledig) in kaart te brengen en te analyseren, en een adequaat en passend privacybeleid te hanteren. Ook bestaat het risico dat in het geval van incidenten, de organisatie niet op adequate wijze weet te handelen omdat het simpelweg geen inzicht heeft in de verwerkingen van haar persoonsgegevens. Verder kan er geen gedocumenteerde verantwoording aan de toezichthouder worden overlegd als deze daar om vraagt. Een algemeen risico is de organisatie reputatieschade oploopt en dat de Autoriteit Persoonsgegevens (hoge) boetes kan opleggen.
4	***(Sub)verwerkers en verwerkersovereenkomsten***	Een organisatie is verplicht om afspraken te maken (vaak in de vorm van verwerkersovereenkomsten) met partijen die ten opzichte van de organisatie (de verwerkingsverantwoordelijke) als verwerker zijn te kwalificeren. Daarbij gaat het om persoonsgegevens, afkomstig van de betrokkenen van de verwerkingsverantwoordelijke, die in het kader van het (sub)verwerkerschap worden verwerkt.	Als organisaties ervoor kiezen om gebruik te maken van (sub)verwerkers, dan vereist de AVG dat met deze (sub)verwerkers afspraken worden vastgelegd. Dit gebeurt meestal in de vorm van een verwerkersovereenkomst. Deze overeenkomst moet ervoor zorgen dat de privacy en persoonsgegevens van betrokkenen op afdoende wijze worden beschermd. Als de organisatie niet afdoende haar (sub)verwerkers in kaart brengt en met hen overeenkomsten sluit, loopt zij het risico op ongeoorloofd (her)gebruik, datalekken etc. Dit kan resulteren in reputatieschade en een (hoge) boete, op te leggen door de Autoriteit Persoonsgegevens.

5	***Bewaartermijnen en vernietiging persoonsgegevens***	Persoonsgegevens die door een organisatie worden verwerkt mogen niet onbeperkt bewaard blijven en moeten van een bewaartermijn voorzien zijn. Na het verstrijken van de bewaartermijn moeten de persoonsgegevens worden vernietigd. In dat kader hanteert de organisatie een bewaar- (of archief-) en vernietigingsbeleid. In dit beleid stelt de organisatie vast hoe lang de bewaartermijnen voor de persoonsgegevens zijn en op welke wijze de persoonsgegevens na het verstrijken van de bewaartermijn worden vernietigd.	organisaties zijn verplicht bewaartermijn te hanteren als het gaat om de verwerking van persoonsgegevens. Na het verstrijken van deze bewaartermijnen is een organisatie verplicht de persoonsgegevens te vernietigen. Als de persoonsgegevens niet (op tijd) worden verwijderd, is er onnodig verhoogd risico op datalekken en loopt zij hierdoor het risico op reputatieschade en een (hoge) boete, op te leggen door de Autoriteit Persoonsgegevens.
6	***Rechten van betrokkenen***	De organisatie verstrekt haar betrokkenen, bijvoorbeeld door middel van haar privacyverklaring, informatie over de verwerking van persoonsgegevens. Hierdoor hebben betrokkenen inzicht in de processen en zijn zij staat hun rechten uit te oefenen. Dit moet zonder belemmeringen kunnen, tenzij een specifieke uitzonderingsgrond van toepassing is. In het kader van de mogelijkheid tot uitoefening van de rechten van betrokkenen hanteert de organisatie een beleid waarin is beschreven hoe verzoeken van betrokken om hun rechten uit te oefenen worden behandeld.	Betrokkenen hebben diverse rechten als het gaat om de verwerking van persoonsgegevens die op hen betrekking hebben. Het is de verantwoordelijkheid van de organisatie die deze persoonsgegevens verwerkt om zowel organisatorische als technische procedures binnen de organisatie in te richten om ervoor te zorgen dat betrokkenen hun rechten op effectieve wijze kunnen uitvoeren. Als een organisatie niet een dergelijke procedure heeft geïmplementeerd, loopt zij het risico op onvolledige, ontijdige of onzorgvuldige beantwoording op verzoeken. Hiermee overtreedt zij de wet en loopt zij het risico op reputatieschade en een (hoge) boete, op te leggen door de Autoriteit Persoonsgegevens.

7	***Datalekken- en incidenten***	Een organisatie is verplicht om beleid aangaande datalekken en -incidenten in te richten. Als zich een datalek of -incident voordoet, dan moet de organisatie conform het beleid handelen. Daarbij wordt in ieder geval de Functionaris Gegevensbescherming, indien deze is aangesteld, ingelicht. Na overleg met de FG wordt besloten om het datalek of -incident al dan niet aan de Autoriteit Persoonsgegevens en/of betrokkene(n) te melden. Tevens onderhoudt de organisatie een register waarin datalekken en -incidenten worden opgenomen.	Het is mogelijk dat zich tijdens de verwerking van persoonsgegevens incidenten of datalekken voordoen. Om ervoor te zorgen dat deze incidenten en lekken (zo veel) mogelijk worden beheerst en (reputatie)schade voor betrokkenen en organisatie te beperken, is beleid noodzakelijk.. Ook wordt hierdoor, indien vereist, tijdig de Autoriteit Persoonsgegevens ingelicht. Als een organisatie niet op adequate wijze omgaat met incidenten en datalekken, is er mogelijk groot risico voor betrokkenen en de organisatie zelf. Zij overtreedt dan de wet en loopt het risico op reputatieschade en een (hoge) boete, op te leggen door de Autoriteit Persoonsgegevens. Ook zijn gerechtelijke procedures mogelijk.
8	***Bewustwording, kennis en training***	De interne stakeholders van de organisatie worden op passende wijze, in relatie tot hun functie en rol, bewust gemaakt en getraind met betrekking tot het omgaan met persoonsgegevens. Zij worden bijgeschoold als er veranderingen zijn in wet- en regelgeving, standaarden en/of gesignaleerde tekortkomingen, voor zover relevant voor de uit te oefenen functie. In dit proces wordt advies gevraagd aan de Functionaris Gegevensbescherming.	Bewustwording en kennisvergaring (door middel van training) zijn essentieel voor het beheersen van privacy- en informatiebeveiligingsrisico's. Als dit niet het geval is, loopt de organisatie het risico dat zij daardoor rechten van betrokkenen schaadt en de wet overtreedt. Hierdoor bestaat het risico op reputatieschade en een (hoge) boete, op te leggen door de Autoriteit Persoonsgegevens.

9	***Technische en organisatorische maatregelen (informatiebeveiligingsbeleid)***	Een organisatie is bij de verwerking van persoonsgegevens verplicht passende technische en organisatorische maatregelen te nemen om de persoonsgegevens op te beschermen. De beschrijving van deze maatregelen staat in het informatiebeveiligingsbeleid. Het privacybeleid en informatiebeveiligingsbeleid kunnen een gecombineerd en integraal beleid zijn. Bij het opstellen van het beleid houdt de organisatie rekening met de huidige stand van de techniek, de (uitvoerings)kosten, maar ook met de aard, de context en het doel van de verwerking en privacyrisico's voor de rechten en vrijheden van de betrokkenen. In dat kader wordt aan gesloten bij algemeen geaccepteerde beveiligingstandaarden binnen het domein van informatiebeveiliging, zijnde op dit moment ISO 270001, ISO 270002, ISO 27701, BIO, NEN7510 en NTA7516. Een essentiële technische en organisatorische maatregel is het opstellen van een autorisatiematrix. Dit is een manier om inzichtelijk te maken welke interne stakeholders geautoriseerd zijn om welk persoonsgegevens te verwerken. Daarbij mogen uitsluitend interne stakeholders toegang hebben tot persoonsgegevens als dit noodzakelijk is voor het uitoefenen van hun functie. Ten aanzien van de	Het vastleggen en hanteren van beleid is een vorm van zelfbinding en kwaliteitswaarborging. Indien een verwerkingsverantwoordelijke geen informatiebeveiligingsbeleid vastlegt en hanteert, dan kan zij niet (op afdoende wijze) de privacy van betrokkenen waarborgen. Binnen de organisatie is niet beschreven op welke wijze de organisatie omgaat met de beveiliging van (persoons)gegevens. Als gevolg daarvan kan de kwaliteit van de dienstverlening/product van de organisatie niet (afdoende) worden gewaarborgd. Tevens bestaat het risico dat in het geval van incidenten, de organisatie niet op adequate wijze weet te handelen omdat het simpelweg geen beleid heeft om de incidenten te beheersen. Een algemeen risico is dat de organisatie reputatieschade oploopt en dat de Autoriteit Persoonsgegevens (hoge) boetes kan opleggen. Onderdeel van het nemen van passende technische en organisatorische maatregelen is het inregelen van de juiste autorisaties, meestal vastgelegd in een autorisatiematrix. Het ontbreken van onderbouwde toekenning van autorisaties en de vastlegging daarvan in een autorisatiematrix, brengt het risico met zich mee dat onbevoegden toegang verkrijgen tot persoonsgegevens. Daarmee loopt de organisatie het risico dat betrokkenen worden geschaad en dat zij

		autorisaties worden in ieder geval de volgende aspecten ingeregeld: - Toekennen en beheer van toegangsrechten (vastgelegd in een autorisatiematrix); - Beschrijving functieprofielen en bijbehorende gebruikersrollen.	daardoor de wet overtreedt. Dit kan leiden tot een risico op reputatieschade en een (hoge) boete, op te leggen door de Autoriteit Persoonsgegevens.
10	***Data protection impact assessment (DPIA)***	In sommige gevallen is het verplicht, dan wel aan te raden, voor een organisatie om een Data Protection Impact Assessment (DPIA) of Gegevensbeschermings-effectbeoordeling (GEB) uit te voeren. Door middel van een DPIA wordt op een gestructureerde en duidelijke wijze privacyrisico's (van een bepaalde verwerkingsactiviteit) voor betrokkenen inzichtelijk gemaakt. Bij het uitvoeren van een DPIA wordt de Functionaris Gegevensbescherming altijd betrokken. In het kader van de DPIA heeft de organisatie een beleid opgesteld. Dit beleid kan een onderdeel zijn van het algemene privacybeleid of een opzichzelfstaand beleidsstuk zijn. In een dergelijk beleid wordt (onder andere) opgenomen in welke gevallen een organisatie een DPIA uitvoert en hoe het evaluatie- en actualisatieproces van de DPIA eruit ziet.	Data Protection Impact Assessments (DPIA's) zijn een instrument voor organisatie om (specifieke) privacyrisico's in kaart te brengen en, indien nodig, deze te beheersen. Indien de organisatie geen DPIA's verricht en herziet, dan wel geen beleid daarvoor hanteert, loopt zij het risico dat de privacyrisico's voor haar betrokkenen onvoldoende in kaart zijn gebracht. Daardoor kan sprake zijn van een niet afdoende bescherming van de privacy van betrokkenen, die uiteindelijk weer kan leiden tot reputatieschade schade voor de organisatie en een (hoge) boete, op te leggen door de Autoriteit Persoonsgegevens.