AVG GAP-ANALYSE

Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Op dat moment beschermen wij de privacy van onze gegevens niet meer op basis van de Nederlandse Wet bescherming persoonsgegevens (Wbp), maar op basis van een Europese privacyverordening.

Veel van de wetgeving die is opgenomen in de AVG is al onderdeel van de Wbp. Maar op diverse onderwerpen introduceert de AVG veranderingen of nieuwe verplichtingen. Zo hoeven persoonsgegevens verwerkende organisaties geen melding meer te doen van hun verwerking bij de Autoriteit Persoonsgegevens (voorheen het CBP), maar dienen zij wel zelf een verwerkingsregister bij te houden. De AVG verandert de (passieve) registratieplicht hiermee in een (gedetailleerdere en continu te onderhouden) documentatieplicht waarmee organisaties actief moeten aantonen de privacyregels na te leven. In eerste instantie naar zichzelf toe, maar bij controle ook richting de Autoriteit Persoonsgegevens (AP). Ook krijgen betrokkenen (de personen van wie gegevens worden verwerkt en beschermd) met het van toepassing worden van de AVG meer rechten. Bijvoorbeeld daar waar het om het verwijderen, bevriezen, corrigeren en porteren van de over hen verwerkte persoonsgegevens gaat. De gewijzigde rechten van de betrokkenen hebben tezamen met de documentatieplicht vermoedelijk de grootste impact op organisaties.

Checklist

Om een goede pragmatische start te maken met de nieuwe wetgeving is bij dit artikel een checklist gevoegd die voor een GAP-analyse kan worden gebruikt. Als je als organisatie reeds eerder aandacht besteedde aan de Wbp, weet je op basis van de checklist snel aan welke onderwerpen nog aandacht moet worden besteed bij het van toepassing worden van de AVG. Van deze checklist is op classity.nl ook een online versie beschikbaar, inclusief verwijzingen naar de relevante AVG-artikelen voor meer informatie. De resultaten zijn bij het gebruik van de site na het invullen als pdf te downloaden. Deze pdf bevat bij een zorgvuldige beantwoording ook meteen een goede start voor het opzetten van het verplichte verwerkingsregister.
Voldoe ik hiermee volledig aan de AVG? Nee. Het is niet mogelijk om met een enkele actie volledig aan de AVG te voldoen. De AVG vereist dat je controle hebt én houdt over je verwerking. Dit vereist een continue proces. Je voldoet dus niet aan de AVG als je eenmalig een activiteit voltooit, maar pas als je aan kunt tonen over een langere periode verantwoord met persoonsgegevens om te kunnen gaan.

Daarnaast is er geen 'one size fits all'-aanpak voor het voldoen aan de AVG. Hiervoor laat de wet teveel ruimte voor interpretatie. De wet zal de komende tijd verder gepolijst worden met zienswijzen (waarin de Europese toezichthouders uitleggen hoe zij de wet interpreteren) en jurisprudentie. Organisaties die een zeer behoudende koers varen, zullen de teugels op basis van deze ontwikkelingen in de toekomst mogelijk een beetje kunnen laten vieren. En organisaties die de wet heel vrij interpreteren moeten vermoedelijk naderhand een tandje bijzetten. Kortom, de GAP-analyse is bedoeld om een vliegende start te maken met de belangrijkste onderwerpen. Voor organisaties die nog niet zijn gestart, kan dit vermoedelijk geen kwaad. Want het is 25 mei 2018 voor we er erg in hebben.

Maarten Hartsuijker is consultant en ethisch hacker bij Classity en helpt organisaties in de volle breedte met informatiebeveiliging (en privacy). Maarten is tevens redacteur bij IB-Magazine. Hij is bereikbaar via m.hartsuijker@classity.nl.

Checklist

Doelstelling	GAP?	Benodigde actie	Benodigde resources
WETTELIJKE GRONDSLAG			
De wettelijke grondslag voor de verwerking is vastgesteld en vastgelegd (bijv.: vanuit overeenkomst, toestemming, gerechtvaardigd belang)			
Persoonsgegevens worden alleen verwerkt voor het doel waarvoor ze primair zijn afgestaan. Voor andere doelen is aanvullende ondubbelzinnige toestemming verkregen en vastgelegd, tenzij er andere grondslagen zijn die een verwerking rechtvaardigen (zoals een gerechtvaardigd belang of een wettelijke plicht). Bij het vragen van ondubbelzinnige toestemming zijn klanten goed geïnformeerd over waarvoor zij exact toestemming verlenen.			
DOCUMENTEREN			
Bij de verwerking van persoonsgegevens wordt geregistreerd: - wie er verantwoordelijk is; - wat het doel van de verwerking is; - welke categoriën betrokkenen er zijn (klanten/medewerkers/etc.); - welke categoriën persoonsgegevens er verwerkt worden (NAW/Financieel/locatie/etc.); - welke derden er betrokken zijn bij de verwerking, - of er persoonsgegevens worden doorgegeven aan 'derde landen' buiten de EU; - wat de bewaartermijnen zijn; - welke technische-organisatorische beschermingsmaatregelen er getroffen zijn.			
Bij het vragen van toestemming voor een specifieke verwerking wordt geregistreerd: - Waar toestemming voor is gegeven; - Waar en wanneer de toestemming is gevraagd; - Hoe de toestemmingsvraag is gesteld (en waarover is geïnformeerd).			
Indien de verwerking van bijzondere categorieën van persoonsgegevens (medisch/etniciteit/geloofsovertuiging/etc.) noodzakelijk en gerechtvaardigd is, is altijd een uitdrukkelijke (expliciete) toestemming gevraagd en vastgelegd (de uitdrukkelijke toestemming is tevens ondubbelzinnig).			
Er ligt vast voor welke gegevens een specifieke wettelijke bewaarplicht geldt. Deze bewaarplicht wordt bij een verzoek tot gegevenswissing niet uit het oog verloren.			
Van gegevens van kinderen is de toestemming van de ouder of voogd vastgelegd. Met alle partijen waarmee wordt samengewerkt is (in samenspraak met de juristen) een verwerkersovereenkomst afgesloten.			
De organisatie is transparant over de wijze waarop de persoonsgegevens worden verwerkt, o.a. door goede communicatie via het privacy statement.			
RECHTEN BETROKKENEN			
De gegevens die over een persoon verzameld zijn kunnen op verzoek binnen 4 weken worden gewist.			
Op verzoek kan binnen 4 weken een kopie van de over iemand verwerkte persoonsgegevens worden aangeleverd, inclusief de doelen waarvoor de gegevens verzameld zijn.			
Aan te leveren kopieën zijn in een uniform, voor machines leesbaar formaat, beschikbaar. Gegevensverwerkingen kunnen voor specifieke personen (binnen 4 weken) worden opgeschort op het moment dat daar recht op is ('blokkeren' van mutaties / bevriezen van de gegevens). Doorgegeven actualisaties of correcties van persoonsgegevens kunnen binnen 4 weken worden doorgevoerd.			
Voordat persoonsgegevens worden verstrekt (geldt ook voor: corrigeren/actualiseren/ verwijderen/blokkeren) wordt altijd de identiteit van de persoon die dit verzoekt vastgesteld. Hierbij wordt rekening gehouden met eventuele uitzonderingen en vastgelegde machtigingen.			

Doelstelling	GAP?	Benodigde actie	Benodigde resources
Verzoeken tot correctie/actualisatie/ verwijdering/opschorting van (het gebruik van) persoonsgegevens kunnen overal worden doorgevoerd, ook als verwerkingen aan andere afdelingen, organisatieonderdelen of derden zijn uitbesteed. Hierbij wordt rekening gehouden met verplichtingen uit andere / meer zwaarwegende regelgeving. Denk aan langere bewaarverplichting als gevolg van belastingwetgeving voor specifieke financiële gegevens.			
Binnen systemen en processen waarin geautomatiseerd wordt geprofileerd is het mogelijk om specifieke personen (die dit aangeven) van deze geautomatiseerde verwerking uit te sluiten. We spreken van profilering indien beslissingen enkel op een geautomatiseerde verwerking zijn gebaseerd (data analytics, big data).			
Er is gefaciliteerd dat een verstrekte toestemming voor het verwerken van persoonsgegevens door een persoon net zo makkelijk kan worden ingetrokken als dat hij is afgegeven.			
PRIVACY BY DESIGN / DEFAULT			
Persoonsgegevens verwerkende systemen en processen zijn privacy-vriendelijk ontworpen en standaard staan verwerkingsinstellingen (waaronder toestemmingen) zo privacy-vriendelijk mogelijk ingesteld. (privacy by design, privacy by default).			
Er is een PIA uitgevoerd indien de verwerkingsactiviteiten een hoog risico voor de betrokkenen met zich mee kan brengen. Dit is het geval indien: - nieuwe technologie wordt geïmplementeerd; - er grote hoeveelheden persoonsgegevens worden verwerkt; - er bijzondere persoonsgegevens worden verwerkt - wanneer er gebruik wordt gemaakt van geautomatiseerde besluitvorming en deze een aanzienlijk effect teweeg kan brengen voor betrokkenen.			
Gegevens worden niet langer dan noodzakelijk is bewaard.			
Indien het voor een specifieke verwerking niet noodzakelijk is dat gegevens tot op de persoon herleidbaar zijn, zijn anonimisatietechnieken toegepast.			
Gegevens die worden ingezet om de dienstverlening te optimaliseren, te testen en om producten te verbeteren, worden daarvoor geanonimiseerd. (Indien het met geanonimiseerde data niet mogelijk is om dit doel te bereiken kan het met de juiste privacywaarborgen ook te verantwoorden zijn om geen anonimisatie- maar pseudonimisatietechnieken in te zetten).			
Alle maatregelen die volgen uit het beveiligingsbeleid (en de daarvan afgeleide baseline) zijn toegepast.			
PRIVACYORGANISATIE			
Er is een privacy officer aangesteld met voldoende kennis en steun en mandaat van het bestuur om de verantwoordelijkheid voor het borgen van een passende bescherming van persoonsgegevens op zich te nemen.			
Het privacybeleid houdt rekening met de uitgangspunten uit de AVG en beschrijft hoe de privacyrollen en verantwoordelijkheden in de organisatie zijn belegd.			
Het beveiligingsbeleid houdt rekening met de uitgangspunten uit de AVG en beschrijft hoe de beveiligingsrollen en verantwoordelijkheden in de organisatie zijn belegd Er is vastgelegd op welke wijze een datalek kan worden afgehandeld. Er is vastgelegd op welke wijze er invulling wordt gegeven aan werkzaamheden die gerelateerd zijn aan betrokkenen die gebruik maken van hun rechten (inzien/verwijderen/muteren/bevriezen/bezwaar tegen profilering).			