Stappenplan naar GDPR compliance

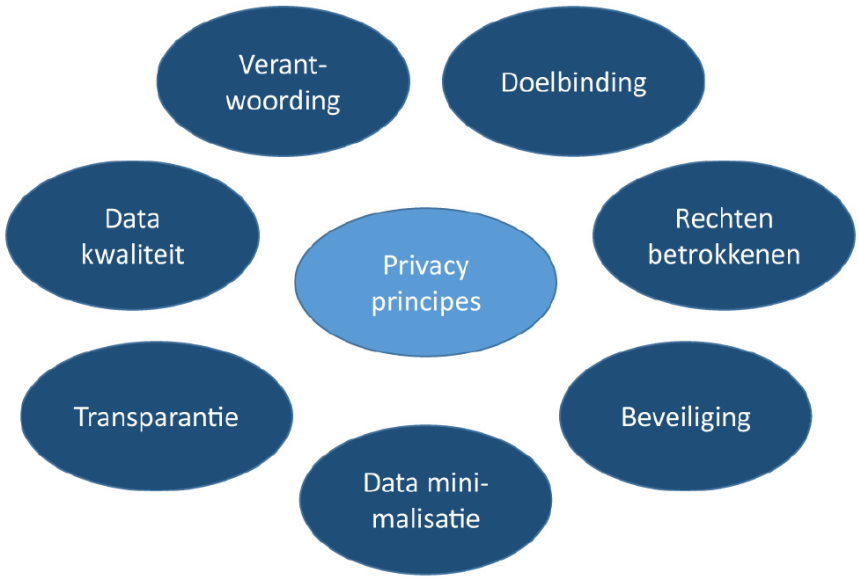
Stappenplan voor compliance met de Algemene Verordening Gegevensbescherming

Het Europees Parlement heeft op 14 april 2016 de Algemene Verordening Gegevensbescherming (AVG) vastgesteld. De AVG vervangt de eerdere EU verordening uit 1995, de Data Protection Directive 95/46/EC. De AVG heeft significante gevolgen voor organisaties en de door hen gebruikte IT systemen. De verordening heeft directe werking in de lidstaten van de Europese Unie. Daarbij hebben lidstaten tot uiterlijk 25 mei 2018 de tijd om de verordening in te voeren en over te gaan tot handhaving. Vrijwel elke organisatie moet voor die tijd maatregelen treffen om aan de eisen van de AVG te voldoen. Het niet voldoen aan de AVG kan leiden tot boetes die kunnen oplopen tot €20 miljoen of 4% van de wereldwijde jaaromzet.

Naleving van privacy principes moet individuen beschermen

De AVG vindt haar basis in de privacy principes beschreven in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM). In 2013 heeft de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO) de definities van de zogenaamde informationele privacy principes geactualiseerd. Uitgangspunt in de AVG is dat elke gedigitaliseerde verwerking van persoonsgegevens een inbreuk vormt op de persoonlijke levenssfeer van de betrokkenen. De verantwoordelijke organisatie moet aantonen dat organisatorische en technische maatregelen zijn getroffen waarmee invulling is gegeven aan de privacy principes en de risico's voor betrokken zijn geminimaliseerd.

Stappenplan voor compliance met de Algemene Verordening Gegevensbescherming



Schema: Privacy principes ter bescherming van klanten, burgers en consumenten

Digitalisering en privacybescherming zijn maatschappelijke en bestuurlijke thema's en raken mensenrechten. Veel organisaties zien dat het voldoen aan de AVG om marktreputatie gaat en privacybescherming een onderdeel is van maatschappelijk verantwoord ondernemen. Compliance met de AVG is meer en meer een voorwaarde voor deelname aan de gedigitaliseerde samenleving en economie.

Met alleen papieren maatregelen lukt het niet

De AVG stelt onder meer dat organisaties de beveiliging, integriteit, authenticiteit en beschikbaarheid van persoonsgegevens permanent moeten garanderen. Dit vereist naast organisatorische vooral ook technologische maatregelen. Op dit punt wijkt de AVG af van de vorige privacy verordeningen. De focus ligt veel meer op de maatregelen in de IT: de IT werkelijkheid. Met alleen organisatorische en procedurele maatregelen is het niet mogelijk om aan de AVG te voldoen.

Artikel 32 van de AVG stelt dat de verantwoordelijke organisatie de beveiliging van persoonsgegevens permanent moet garanderen door organisatorische én technische maatregelen te treffen. De beveiliging betreft de vertrouwelijkheid, de integriteit en de beschikbaarheid van de verwerking van data. De organisatie dient bovendien maatregelen te hebben geïmplementeerd om beveiligingsincidenten en datalekken tijdig te detecteren en de gevolgen voor betrokkenen te minimaliseren. Door periodiek testen, beoordelen en evalueren van de beveiliging moet de werking van de beveiliging worden aangetoond.

Een andere technische aanwijzing uit de AVG is dat de **beveiligingsmaatregelen naar de laatste stand van de techniek moeten** zijn ingericht. De AVG spreekt van het toepassen van pseudonimisering en **versleuteling**. Pseudonimisering en **versleuteling** van persoonsgegevens zijn sterke maatregelen om de risico's van datalekken en ook de risico's van profiling te beperken. In het bijzonder wordt gewezen op de risico's van het opslaan en verwerken van digitale identifiers en wachtwoorden. Hiervoor zijn aanvullende maatregelen nodig zoals versleuteling en **segmentering van systemen** of het offline opslaan van gegevens. De eis dat de beveiliging permanent gegarandeerd moet kunnen worden, maakt ook duidelijk dat er zowel **preventieve, als detectieve maatregelen** nodig zijn. Het gebruik van security logging en het periodiek analyseren van logging zijn belangrijke randvoorwaarden om de werking van beveiligingsmaatregelen aan te kunnen tonen. Afhankelijk van de gevoeligheid van de verwerking zullen ook technologieën als **intrusion detection en prevention en monitoring** systemen overwogen moeten worden.

Nederland loopt voorop met de invoering: meldplicht datalekken

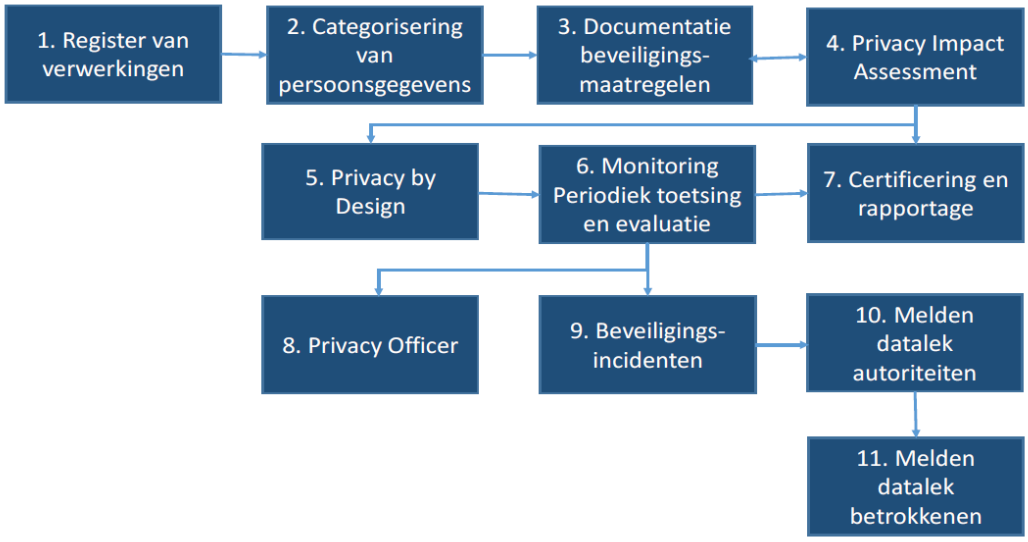
Vooruitlopend op de invoering van de AVG heeft Nederland per 1 januari 2016 de meldplicht datalekken ingevoerd. Dit is een onderdeel van de AVG en beschreven in artikel 33 en 34. Hiermee loopt Nederland voorop in Europa met de invoering. Met sancties die kunnen oplopen tot 10% van de jaaromzet is ook een sterk signaal afgeven waarmee het belang van naleving van de nieuwe verordening is onderstreept. De meldplicht houdt in dat in geval van een onrechtmatige verwerking of onrechtmatige toegang tot persoonsgegevens dit gemeld moet worden bij de Autoriteit Persoonsgegevens en ook aan alle betrokkenen indien zij nadelige effecten hiervan kunnen ondervinden. Melding aan de autoriteiten dient onverwijld en uiterlijk binnen 72 uur te geschieden.

Melding aan betrokkenen kan achterwege blijven indien de verantwoordelijke organisatie aantoonbare toereikende technische beveiligingsmaatregelen heeft getroffen waardoor de gevolgen voor de betrokkenen geminimaliseerd zijn. **Versleuteling, segmentering, logging van security incidenten, sterke authenticatie mechanismen en ondersteunende maatregelen als monitoring en periodieke controle** zijn in dit verband zinvolle maatregelen. In geval van een datalek is het belangrijk dat een organisatie kan aantonen dat zij de benodigde beveiligingsmaatregelen op orde heeft. Hiermee kunnen hoge boetes worden voorkomen en kosten worden vermeden om achteraf de gevolgen van een datalek te minimaliseren. Documentatie van beveiligingsmaatregelen is ook daarom belangrijk. Er geldt **een bewaarplicht voor de documentatie van security** incidenten en datalekken.

Een inbreuk middels malware dient altijd gemeld te worden bij de autoriteiten. Het aantreffen van malware op een systeem wordt gezien als het verlies van controle over dat systeem door de verantwoordelijke. Malware prevention en malware detection in combinatie met segmentering van netwerken kunnen effectieve maatregelen zijn ter beperking van de gevolgen van malware.

Handreiking roadmap voor compliance met de AVG

Hieronder volgt een highlevel stappenplan waarin is aangegeven welke stappen zoal doorlopen moeten worden om aan de AVG te kunnen voldoen.



Schema: Privacy principes ter bescherming van klanten, burgers en consumenten

1. **Register van verwerkingen (WP par 2.1.1, blad 9 / Artikel 30 AVG)**

   Leg een register aan van alle verwerkingen van persoonsgegevens, dit register bevat per verwerking het doel en de aard van de verwerking, de getroffen beveiligingsmaatregelen en wie verantwoordelijk is.

2. **Categorisering van persoonsgegevens (WP par 2.1.1, blad 9 / Artikel 9 AVG)**

   Geef aan wat de gevoeligheid van de verwerkte persoonsgegevens zijn en welke risico's hiermee gemoeid zijn voor de betrokkenen.

3. **Documentatie beveiligingsmaatregelen (WP par 2.2.2, blad 10 / Artikel 30, 32 AVG)**

   Zorg voor een beschrijving van de technische en organisatorische maatregelen zoals die zijn gerealiseerd.

4. **Privacy Impact Assessment (WP par 2.2, blad 8 / Artikel 35 AVG)**

   Toets periodiek of getroffen maatregelen nog in lijn zijn met de AVG en met alle privacy principes en risico's en of de doelstelling van de verwerking behaald kan worden via andere wegen of met minder persoonsgegevens. Voer bij gewijzigde omstandigheden of wijzigingen in systemen een privacy Impact assessment uit.

5. **Privacy by Design (WP par 2.2.8, blad 15 / Artikel 35 AVG)**

   Bij invoering van nieuwe verwerkingen van persoonsgegevens of bij wijzigingen zorg dat vanaf het begin ontwerpcriteria worden gehanteerd waarmee invulling kan worden gegeven aan het principe van "privacy by design". Systemen dienen voordat deze in gebruik worden genomen naar de laatste stand van de techniek zijn beveiligd.

6. **Monitoring, periodieke toetsing en evaluatie (WP par 2.1.1, blad 9 / artikel 30, 32 AVG)**

   Implementeer technische middelen en organisatorische procedures die waarborgen dat de beveiliging van systemen en de daarmee verwerkte persoonsgegevens permanent gegarandeerd wordt. Richt een management cyclus in waarbij zo nodig optimalisaties worden doorgevoerd.

7. **Certificering en rapportage (WP par 2.1.1, blad 9 en 10 / artikel 42 AVG)**

   Maak verwerkingen en gerealiseerde beschermingsmaatregelen transparant. Overweeg om stakeholders periodiek te informeren over de gerealiseerde beveiliging van persoonsgegevens en de privacy impact assessment rapportages.

8. **Privacy Officer / Functionaris voor de gegevensbescherming (WP par 1.3, blad 6 / artikel 37 AVG)**

   Stel als de criteria daartoe bereikt zijn een functionaris voor de gegevensbescherming aan.

9. **Beveiligingsincidenten (WP par 3.9, blad 21 / AVG artikel 33, 34)**

Implementeer maatregelen om beveiligingsincidenten te detecteren en de gevolgen daarvan te beperken. Zorg voor documentatie van incidenten.

10. **Melden datalek bij autoriteiten (WP par 3.9, blad 21 / AVG artikel 34)**
    Richt een procedure meldplicht datalekken in waarmee datalekken worden gedetecteerd en aan de Autoriteit Persoonsgegevens binnen 72 uur worden gemeld. Zorg voor documentatie van datalekken.
11. **Melden datalek bij betrokkenen (WP par 3.9, blad 21 / AVG artikel 34)**
    Implementeer een procedure waarmee indien een datalek nadelige gevolgen heeft voor betrokkenen, deze betrokkenen onverwijld geïnformeerd kunnen worden over het gesignaleerde datalek.

Zoekt u hulp of advies aangaande de gevolgen voor u of uw klanten?

Neem gerust contact met ons op:

Jan-Hendrik Straatman – Director Sales & Marketing
jan-hendrik.straatman@beeone.nl
Marysia Houben – Accountmanager
marysia.houben@beeone.nl
Math Leise – Manager Inside Sales & Product and Service Development
math.leise@beeone.nl
Tom Heusschen – Inside Sales Employee
tom.heusschen@beeone.nl

Wij zijn tevens bereikbaar op: 046 457 26 86