



## AANTOONBAAR 'IN CONTROL' DOOR BORGING VAN DE AVG/GDPR

Mavim AVG/GDPR framework

Het is belangrijk dat organisaties hun privacygevoelige gegevens beschermen. Niet alleen om identiteitsfraude, imago- en financiële schade te voorkomen, maar ook om te voldoen aan de privacywetgeving. Daarom is de Algemene Verordening Gegevensbescherming (AVG), ook bekend als de General Data Protection Regulation (GDPR) in het leven geroepen. De verordening dient ertoe het recht te beschermen op zorgvuldige behandeling van persoonlijke gegevens door organisaties en om zelf te bepalen wie welke persoonsgegevens krijgt.

### WAT IS ER NIEUW?

Naast een herziening van bestaande regelgeving bevat de AVG/GDPR een aantal nieuwe richtlijnen. De nieuwe elementen hebben betrekking op:

- ▶ Verwerkingsregister
- ▶ Privacy by design | Privacy by default
- ▶ Strengere regels rond profilering
- ▶ Uitvoering van privacy impact assessments (PIA)
- ▶ Recht om vergeten te worden
- ▶ Dataportabiliteit (recht op overdraagbaarheid van persoonsgegevens)
- ▶ Plicht tot informeren van betrokkenen
- ▶ Uitbreiding van de rechten van betrokkenen

### REGELGEVING GEBORGD

De borging van de AVG-regelgeving is voor organisaties die persoonsgegevens beheren, verzamelen of verwerken van essentieel belang. Hiermee kunnen organisaties immers beter inspelen op veranderingen en aanvragen, kunnen zij aantonen dat zij 'in control' zijn, voldoen organisaties aan hun verplichting jegens hun klanten en kunnen organisaties hoge boetes vanuit de Autoriteit Persoonsgegevens voorkomen. Om organisaties te helpen bij het zorgvuldig borgen van de AVG/GDPR, hebben Mavim en Audittrail het AVG/GDPR framework ontwikkeld.

### MAVIM AVG/GDPR FRAMEWORK

Het Mavim AVG/GDPR framework biedt organisaties een ultiem hulpmiddel om enerzijds alle informatie en regelgeving rond de AVG/GDPR vast te leggen en onderling te verbinden en anderzijds om alle informatie en instructies richting medewerkers te communiceren door middel van publicatie via de Mavim Portal.

### NORMENKADER

Het AVG/GDPR framework bevat namelijk alle 99 artikelen van de AVG/GDPR, met daaraan de 173 verordeningen gekoppeld en waarbij bij elk artikel de

### DE VOORDELEN:

- ▶ Overzicht, inzicht en samenhang door verbinding van wetgeving aan processen, mensen, systemen en risico's
- ▶ Duidelijkheid omtrent de status en de mate van beheersing
- ▶ Continu verbeterde compliancy aan de wetgeving door middel van de PDCA cyclus
- ▶ Aantoonbaar in control en transparant richting toezichthouders, zowel intern als extern
- ▶ Eenvoudig inspelen op veranderingen door inzicht en overzicht door relateren van onderwerpen

omschrijving van het artikel is opgenomen. De organisatie kan vervolgens per artikel aangeven wat de status is. Door middel van statusoverzichten wordt vervolgens inzicht verschaft in hoe de organisatie ervoor staat.

#### PRIVACYBELEID EN MELDP LICHT DATALEKKEN

Het privacybeleid van de organisatie kan eenvoudig in het framework worden vastgelegd en gekoppeld aan het normenkader. In het kader van het verwerkingsregister biedt het framework de mogelijkheid om alle relevante processen vast te leggen en door middel van het gebruik van velden het type persoonsgegevens, de proceseigenaren, grondslagen, gebruikte applicaties (waarin persoonsgegevens worden verwerkt) en risicoklassen aan te geven.

Aan de hand van deze informatie kunnen rapporten worden gegenereerd van het verwerkingsregister, risico- en impactanalyses, risico-overzichten, incidentenbeheer en beheersmaatregelen die standaard in het framework zijn opgenomen.

#### BIV-CLASSIFICATIE

Tevens kunnen BIV-classificaties (beschikbaarheid, integriteit en vertrouwelijkheid) op informatie, applicaties en systemen worden toegekend. Deze classificaties dienen als input voor de te nemen maatregelen ter beveiliging van (persoons)gegevens.

In de publicatieportal kan vanuit de BIV-classificatie eenvoudig worden genavigeerd naar de onderliggen-

de processen, functies, rollen, externe stakeholders, het verwerkingsregister en de rechten van betrokkenen. De koppeling met Power BI voorziet in de mogelijkheid om hierop dashboards te genereren.

#### PDCA

Het inregelen van alle zaken rond privacy is geen eenmalige exercitie en behoeft continu verbetering. Ook hieraan kan met behulp van het Mavim AVG/GDPR framework eenvoudig invulling worden gegeven. Door middel van notities en formulieren in een persoonlijk dashboard kunnen namelijk taken en acties worden uitgezet en gemonitord in het kader van de Plan, Do, Check, Act cyclus.

#### KANSEN EN MOGELIJKHEDEN

De implementatie van de AVG/GDPR is beslist geen sinecure en vergt het nodige van organisaties, klein en groot. Anderzijds biedt het organisaties vooral ook om de concurrentie een stap voor te zijn of te blijven.

Om organisaties te helpen bij een goede inrichting en inbedding van de verordening bieden wij niet alleen het Mavim AVG/GDPR framework, maar ook een **whiteteper** waarin de vijf stappen om te voldoen aan de AVG/GDPR uitgebreid staan beschreven. Daarnaast bieden wij een **Quickstart AVG/GDPR implementatie** om uw organisatie te helpen met het in kaart brengen van uw privacy-niveau (in het Mavim AVG/GDPR framework), zodat u een duidelijk en overzichtelijk vertrekpunt heeft.

