mavim
change it

WHITEPAPER

IN 5 STAPPEN VOLDOEN AAN DE GDPR

WHITEPAPER

De wereld van vandaag wordt gekenmerkt door de snelle ontwikkeling van nieuwe technologieën en disruptieve marktomstandigheden. Deze ontwikkelingen hebben verregaande gevolgen voor bestaande organisaties. Om hun bestaansrecht en een concurrerende positie te blijven behouden, zullen zij in staat moeten zijn om snel en flexibel in te kunnen spelen op veranderingen in de markt. Dat betekent dat organisaties meer moeten gaan digitaliseren, hun producten- en dienstenportfolio beter zullen moeten afstemmen op de behoefte van de klant en meer gebruik zullen moeten maken van innovatieve toepassingen. Voor deze organisaties biedt Mavim een platform dat zowel continue verbeterinitiatieven als bedrijfsbrede transformaties in alle facetten ondersteunt.

In één platform ondersteunt Mavim het beheer en de integratie van zes primaire managementthema's voor succesvolle transformatie. De propositie van Mavim is uniek omdat het organisaties in staat stelt de vertrouwde Microsoft-technologieën te blijven gebruiken (zoals Microsoft Visio, Office365, SharePoint, SQL). Daarmee biedt het een eenvoudige omgeving voor de planning en uitvoering van iedere strategische verandering. De Mavim software is in te zetten bij ieder bedrijfsonderdeel en toe te passen op elk managementvraagstuk. De organisatie bepaalt daarbij zelf het startpunt en kan naar wens en behoefte van de organisatie de toepassing uitbreiden of aanpassen.

Het Mavim platform bevat een integratie met modelleer- en publicatietools als Microsoft Visio en SharePoint, voorziet in het hergebruik van bestaande informatie en wordt gekenmerkt door de unieke functionaliteit waarmee verbanden kunnen worden gelegd tussen alle denkbare elementen en gegevens. Hierdoor is Mavim hét ideale platform om iedere transformatie – klein of groot – te realiseren.

INHOUDSOPGAVE

Verwerkt uw organisatie persoonlijke gegevens van Europese burgers? Is uw organisatie gevestigd in de Europese Unie? Is uw organisatie actief in het leveren van goederen en diensten aan Europese burgers via internet?

Heeft u één of meerdere van deze vragen met 'ja' beantwoord, dan is het raadzaam om na te gaan of de General Data Protection Regulation van toepassing is op uw organisatie en wat u moet doen om te voldoen aan de gestelde regels.
Als u de eerste stappen richting GDPR compliance reeds heeft gezet, dan bent u wellicht verder dan de meeste organisaties. Als u echter nog niet begonnen bent, dan zal het u geruststellen dat het gebruik van Mavim u zal helpen om de mate waarin u al dan niet voldoet aan de GDPR eenvoudig inzichtelijk en aantoonbaar te maken.

Wat is de GDPR en is het van toepassing voor mijn organisatie?

De Europese General Data Protection Regulation is wetgeving die reeds is ingegaan per mei 2016, maar die met ingang van 25 mei 2018 daadwerkelijk van kracht zal worden. Het doel van de GDPR is om consumenten te beschermen en duidelijke richtlijnen te scheppen voor organisaties die persoonlijke gegevens verwerken en opslaan. De GDPR waarborgt dat persoonlijke gegevens met toestemming worden opgeslagen en voor de duur die strookt met de reden waarvoor de gegevens aanvankelijk verkregen zijn.

De aanleiding voor de invoering van de GDPR was de behoefte om wetgeving te uniformeren en om consumenten beter te beschermen. Om bedrijven (in het bijzonder multinationals) duidelijke juridische richtlijnen te geven waarbinnen zij dienen te opereren, heeft de Europese Unie besloten om wetgeving rond de bescherming van data in het leven te roepen die de gehele markt omvat. Bovendien voldeed veel bestaande wetgeving rond de gegevensbescherming niet meer omdat deze waren ingevoerd voor de introductie van nieuwe technologieën zoals de cloud. Met het versterken van gegevensbescherming hoopt de EU dat het vertrouwen van consumenten in deze groeiende digitale economie zal toenemen.

De regelgeving is van toepassing voor alle organisaties die gegevens van Europese ingezetenen of van betrokkenen gevestigd in de EU verzamelen of verwerken. De Europese Commissie beschouwt daarbij persoonlijke gegevens als 'iedere vorm van informatie die betrekking heeft op een individu, of het nu zijn of haar persoonlijke, professionele of publieke leven betreft'. Dit kan van alles zijn: van een naam, thuisadres, foto, e-mailadres, bankgegevens, social media berichten en medische informatie tot het IP adres van zijn of haar computer.

Wat is de impact als je niet voldoet aan de GDPR?

Deze regelgeving gaat gepaard met hoge(re) boetes bij overtreding en geeft de individuele

consument meer zeggenschap over wat bedrijven met hun gegevens mogen doen. De essentie van de wetgeving is de privacy van gegevens voor particulieren te waarborgen. De boetes bij overtreding of het niet voldoen aan de wetgeving kunnen oplopen tot € 20 miljoen of 4% van de wereldwijde omzet (afhankelijk van welk bedrag er hoger is).

Afgelopen jaar heeft IT onderzoeks- en adviesbureau Gartner aan de hand van een strategische veronderstelling voorspeld dat 50% van de bedrijven waarop de GDPR van toepassing is, niet volledig zal voldoen aan de vereisten. De laatste ontwikkelingen doen echter vermoeden dat waarschijnlijk bijna 80% van deze organisaties op de gestelde datum niet (volledig) compliant zal zijn.

Wat betekent dit voor mijn organisatie?

Het is hoogst onwaarschijnlijk dat de Europese Unie iedere organisatie die niet voldoet, zal beboeten. Wat wel waarschijnlijk is, is dat binnen elke branche een of meer marktleiders zware boetes krijgen opgelegd. Het beoogde doel daarvan is natuurlijk om organisaties dusdanig af te schrikken dat zij alles in het werk zullen stellen om aan de wetgeving te voldoen. Kleine overtredingen zullen door de vingers worden gezien zolang de betreffende organisatie aan kan tonen dat zij op weg is om binnen een redelijk tijdsbestek volledig compliant te worden – het sleutelwoord hierbij is “aantoonbaar”.

Mavim biedt een software oplossing die gebaseerd is op Microsoft technologieën en die organisaties helpt om de mate waarin zij voldoen aan de GDPR inzichtelijk en aantoonbaar te maken. Alle relevante gegevens en de organisatorische context (wie is er verantwoordelijk, wat is het doel, waar is het te vinden, etc.) kunnen in Mavim worden opgeslagen en beheerd, waardoor je als organisatie ‘audit-klaar’ blijft. Als inzichtelijk is wie wat doet, wanneer en op welke manier, dan is het voor de auditor al snel duidelijk of de organisatie reeds voldoet of op weg is naar volledige compliance.

Het vijf stappen plan naar volledige GDPR compliance met Mavim

1) Inrichten van multifunctionele en multidisciplinaire teams

In plaats van te werken in silo’s kun je beter werken in multifunctionele teams om de informatie die door alle gelederen binnen een organisatie stroomt vast te leggen, te verbinden en te visualiseren. Iedere organisatie heeft haar eigen manier om teams samen te stellen die verantwoordelijk zijn voor het voldoen aan wet- en regelgeving. Sommige organisaties vertrouwen uitsluitend op hun risico- en compliance management functies, maar als gevolg van het ingrijpende karakter van deze wet, lijkt het de moeite waard te overwegen om geïntegreerde teams te formeren door zowel business en enterprise ar-

chitecten als proceseigenaren, IT managers en een vertegenwoordiger van de juridische afdeling aan de teams toe te voegen. Het doel hiervan is om te zorgen voor inzicht in de end-to-end business en de IT-werkzaamheden van uw organisatie, en multifunctionele teams kunnen u hierbij helpen.

2) Vastleggen en zichtbaar maken van persoonlijke gegevens

De GDPR richt zich sterk op persoonlijke gegevens – niet alleen op welke wijze het wordt vergaard, maar ook hoe het verwerkt wordt, wie het verwerkt, waar het wordt vastgelegd en tot wanneer het opgeslagen blijft binnen de organisatie.

Dit vereist een helder overzicht van de huidige manier van werken waarbij gegevens worden gekoppeld aan:

- de bedrijfsprocessen om de procedure voor het omgaan met gegevens en wie de gegevens verwerkt te begrijpen;
- de applicaties en IT-infrastructuur om te begrijpen welke systemen de gegevens verwerken en waar de gegevens worden opgeslagen;
- bedrijfsdoelstellingen om te begrijpen waarom de informatie überhaupt is verkregen en verwerkt;
- de klant-reis-kaarten om de informatiestromen naar en vanuit de organisatie inzichtelijk te maken.

3) Analyseren van het bedrijfsrisico

Nu inzicht is verkregen in alle persoonlijke informatie die door de organisatie stroomt, zult u de risico's en beheersmaatregelen in kaart moeten brengen. Door deze informatie te koppelen aan de end-to-end business en IT activiteiten, kunt u een heat map creëren die de belangrijkste aandachtsgebieden laat zien.

Consensus: Stemt de vastlegging van data overeen met de bepalingen? Kijk naar de klantgerichte processen en systemen. Wordt - waar nodig - duidelijk om toestemming gevraagd? Is het doel van het vastleggen van gegevens aan klanten duidelijk gemaakt? (art. 7).

Bescherming by design: Zijn er adequate controles op de toegang tot persoonlijke gegevens? Is het vergaren van gegevens beperkt tot alleen datgeen wat vereist is voor het doel van de verwerking? (art. 25).

Veilige verwerking: Zijn technische beveiligingsmechanismes voorhanden die bescherming bieden tegen onbevoegd verlies of openbaarmaking van persoonsgegevens? (art. 32).

Delen: Waar worden gegevens gedeeld met derde organisaties of derde landen? Zijn passende controles voorhanden? (art.44-50).

4) Maak uw stappenplan

In de vorige stappen heeft u een holistisch overzicht verkregen van de huidige manier van werken en de mogelijke risico's. Tenslotte kunt u een fit-gap analyse uitvoeren door het gewenste bedrijfsmodel (dat informatie bevat over de gewenste manier van werken, procedures en beheersmaatregelen) in kaart te brengen en te vergelijken met het huidige operationele model. Dit resulteert in output die het bepalen van de stappen, die genomen moeten worden om de aan de GDPR gerelateerde doelstellingen van de organisatie, vergemakkelijkt.

5) Rapporteer, publiceer en monitor

Met Mavim kunt u gedetailleerde rapportages en geavanceerde dashboards genereren van de verbanden tussen risico's en beheersmaatregelen, wetten en regelgeving en bedrijfsprocessen.

Door publicatie via SharePoint / Office365 kunt u de nieuwe processen, risico's, beheersmaatregelen en de onderliggende rollen en systemen eenvoudig communiceren naar eindgebruikers. Bovendien kunnen belanghebbenden de voortgang monitoren en wijzigingen op de bestaande processen controleren in de vertrouwde Microsoft Office-omgeving. Dit helpt bewustwording van de gehele organisatie te creëren en zorgt voor ondersteuning van eindgebruikers en voor het omarmen van de gewenste transformatie.

WAAR KAN MAVIM HELPEN?

Mavim biedt een software oplossing gebaseerd op Microsoft-technologieën en ontworpen om organisaties te helpen informatie over beleid, risico's en regelgeving op geïntegreerde wijze te verbinden en te visualiseren. De bedrijfsprocessen te verbinden met strategie, veranderinitiatieven, risico's, regelgeving en betrokken functionarissen, stelt Mavim organisaties in staat om de impact van risico's op bedrijfsniveau in kaart te brengen en te identificeren.

Het inzicht dat met Mavim gecreëerd wordt, ondersteunt een bedrijfsgedreven en resultaatgerichte aanpak van IT management en bestuur en vergemakkelijkt een eenvoudige naleving zowel richting interne als externe belanghebbenden.

MEER WETEN OVER MAVIM?

- Bezoek onze website of neem contact met ons op via 071 - 364 20 00
- Download de factsheet GDPR met Mavim of bekijk de video
- Vraag geheel vrijblijvend een online demonstratie aan