axians

WHITEPAPER

De impact van de AVG op Data Analytics

Axians
Eemsgolaan 15
9727 DW Groningen
Esp 120
5633 AA Eindhoven
info.bi.nl@axians.com

The best of ICT with a human touch

VINCI ENERGIES

De impact van de AVG op Data Analytics

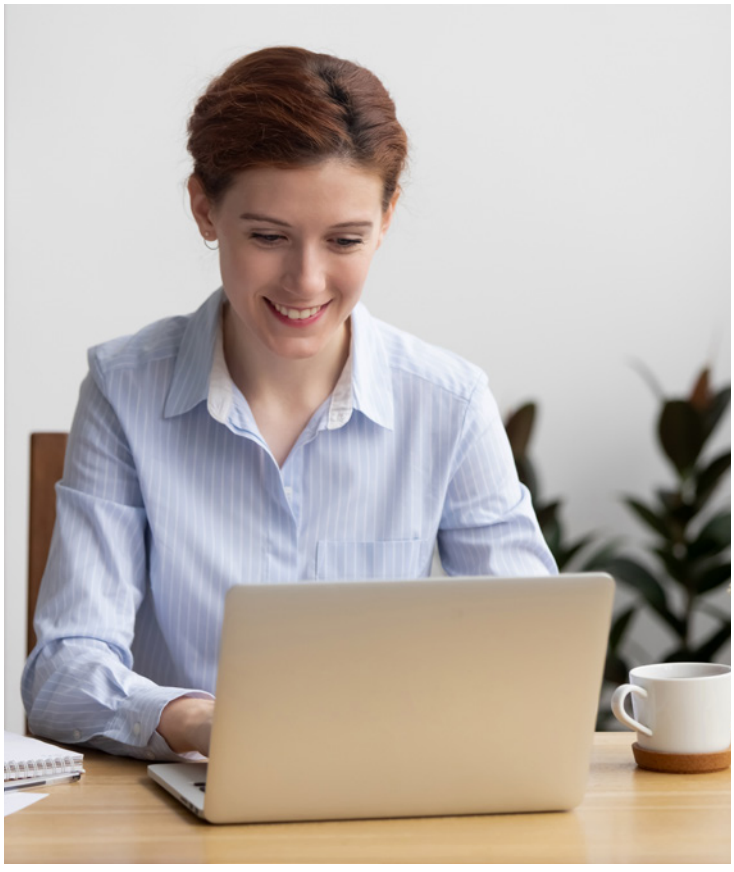
De impact van de Algemene Verordening Gegevens-bescherming (AVG) is voor iedere organisatie anders. De impact is logischerwijs het grootst bij organisaties waar veel met persoonsgegevens wordt gewerkt, zoals ministeries, provincies, gemeenten, zorginstellingen en onderwijsinstellingen.

In het kader van de AVG zijn vaak wezenlijke aanpassingen aan de analytics systemen en processen nodig. Maar wat precies? En hoe pak je dat aan? En hoe zorg je er voor dat je binnen de kaders van AVG toch waarde kunt blijven creëren op basis van data en data-analyse?
Lees er alles over in dit whitepaper.

De AVG & Data Analytics

Bijna iedereen die data verwerkt, krijgt vroeg of laat te maken met de AVG. Deze wet, bedoeld om natuurlijk personen te beschermen bij de verwerking van persoonsgegevens, gaat er vanuit dat verwerking van persoonsgegevens ten dienste staat van de mens. Persoonsgegevens mogen verwerkt worden in een (geautomatiseerd) systeem, maar daarbij moeten wel zeer strikte regels gehanteerd te worden. Voor data analytics wordt geen uitzondering gemaakt.

De AVG is een aantal jaren van kracht. Toch zijn veel organisaties nog steeds op zoek naar mogelijkheden om gegevensets waarin ook persoonsgegevens voorkomen te gebruiken, maar daarbij wel binnen de kaders van de wet te blijven. Voldoen aan de eisen van de AVG, zonder daarbij analytische 'slagkracht' kwijt te raken, is telkens een spanningsveld. Maar ondanks dat niet alles meer kan zijn er diverse methodieken en mechanismen beschikbaar om binnen de wet te kunnen werken met persoonsgegevens.



DATA ALS GRONDSTOF VOOR DE ECONOMIE

Data wordt tegenwoordig gezien als de belangrijkste grondstof van de economie. Slim gebruik van data is de weg naar betere en snellere beslissingen, meer efficiëntie, kostenverlaging, meer flexibiliteit en competitief voordeel. Dataverzameling is niet nieuw, maar de afgelopen jaren heeft technologische vooruitgang ervoor gezorgd dat data op steeds grotere schaal verzamelend, gestructureerd vastgelegd en geanalyseerd worden. In veel gevallen betreft dit ook persoonsgegevens.

Persoonsgegevens
Een persoonsgegeven is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon. Dat betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.

Opslag en analyse van persoonsgegevens zijn vaak gewenst of noodzakelijk vanuit het oogpunt van een optimale dienstverlening naar een eindgebruiker. Maar 'optimale dienstverlening' is een rekbaar begrip. Zo zal het analyseren van patiëntgegevens in een ziekenhuis, ten behoeve van bijvoorbeeld het reduceren van postoperatieve pijn, als gewenst beschouwd worden. Maar wanneer analyse van dezelfde gegevens gebruikt wordt om te bepalen dat een patiënt geen dure medicatie meer krijgt, zal het oordeel heel anders zijn.

Bovendien is bij grootschalige opslag van persoonsgegevens altijd het risico aanwezig dat deze gegevens 'lekken'. Of dat nu is door onoplettendheid, onkunde of diefstal. Juist hierom is de AVG geïntroduceerd: om een einde te maken aan het ongebreideld verzamelen, opslaan en analyseren van data zonder toestemming of welomschreven doel.

BELANGRIJKE UITGANGSPUNTEN VAN DE AVG

De AVG heeft betrekking op de verwerking, het beheer en de beveiliging van persoonsgegevens van Europese burgers. De wet gaat uit van een aantal grondbeginselen bij de verwerking van persoonsgegevens, waarvan rechtmatigheid, doelmatigheid en integriteit en vertrouwelijkheid de kern vormen. Voor een totaaloverzicht verwijzen we je graag naar de website van de Autoriteit Persoonsgegevens (*https://www.autoriteitpersoonsgegevens.nl*)

1. Rechtmatigheid

Rechtmatigheid gaat over de toestemming voor het verwerken van persoonsgegevens van een persoon. De betreffende persoon (ofwel de Betrokkene) moet in de meeste gevallen expliciet toestemming geven voor het verwerken van zijn/haar persoonsgegevens of deze verwerking moet een noodzaak zijn voor het tot uitvoering brengen van een overeenkomst met de Betrokkene. Slechts in enkele gevallen, zoals in het geval van wettelijke verplichtingen of bij een vitaal belang, vervalt deze eis voor expliciete toestemming.

2. Doelmatigheid

Doelmatigheid gaat over de welomschreven doeleinden waartoe persoonsgegevens verwerkt worden. Bij het vragen om toestemming voor verwerking aan de Betrokkene moet duidelijk zijn waarvoor zijn/haar persoonsgegevens gebruikt worden. Vage doeleinden – in de trant van "uw gegevens zullen gebruikt worden om onze dienstverlening aan u te optimaliseren" – zijn ontoereikend.

3. Integriteit en vertrouwelijkheid

Integriteit en vertrouwelijkheid gaan over de manier waarop persoonsgegevens opgeslagen en verwerkt worden. Twee verwante principes zijn daarbij leidend: privacy-by-default en privacy-by-design.

Privacy-by-default

Privacy-by-default houdt in dat alleen die data die nodig zijn voor het specifieke doel opgeslagen en verwerkt worden (dataminimalisatie) en dat deze data alleen opgeslagen worden voor zo lang als nodig is voor dat specifieke doel (retentieminimalisatie).

Privacy-by-design

Privacy-by-design houdt in dat, bij het ontwikkelen van producten of het leveren van diensten, privacy het uitgangspunt is en niet een aspect dat achteraf beoordeeld wordt. Een onderdeel daarvan kan een zogenaamde Data Protection Impact Assessment (DPIA) zijn. Daarbij wordt geïnventariseerd wat de risico's zijn van het verwerken van persoonsgegevens en welke stappen genomen worden om deze risico's te minimaliseren.

Data Protection Impact Assessment (DPIA)

De Autoriteit Persoonsgegevens stelt als vuistregel dat een DPIA verplicht is als gegevens verwerkt worden voor of volgens minstens twee van onderstaande punten:

- Beoordelen van mensen op basis van persoonskenmerken;
- Geautomatiseerde beslissingen;
- Stelselmatige en grootschalige monitoring;
- Gevoelige gegevens;
- Grootschalige gegevensverwerkingen;
- Gekoppelde databases;
- Gegevens over kwetsbare personen;
- Gebruik van nieuwe technologieën;
- Blokkering van een recht, dienst of contract.

FUNCTIONARIS GEGEVENSBESCHERMING

Afhankelijk van het type organisatie of de aard en schaal van de gegevensverwerking is het verplicht om een Functionaris Gegevensbescherming (FG) aan te stellen die bewaakt dat verwerking van persoonsgegevens verloopt volgens de AVG.

VERWERKERSOVEREENKOMST

Het is belangrijk om je te realiseren dat je niet alleen verantwoordelijk bent voor het naleven van AVG in de eigen organisatie. Je moet ook afspraken maken met leveranciers en partners over de naleving. Dat doe je door het afsluiten van een verwerkersovereenkomst. In zo'n verwerkersovereenkomst leg je vast welke persoonsgegevens op welke manier verwerkt worden. Maar ook wat de wederzijdse verantwoordelijkheden zijn en hoe gehandeld dient te worden bij een onverhoopt probleem in de verwerking.

De AVG is een uitdaging voor Analytics

De AVG is specifiek voor het domein van Analytics een grote uitdaging. Analytics is primair gericht op het opleveren van managementinformatie zoals omzet- of verzuimcijfers. Cijfers gepresenteerd op een hoog abstractieniveau dus, waarbij privacy-issues geen rol lijken te spelen. De praktijk is vaak anders. Om te beginnen ligt logica voor het bepalen van deze stuurgetallen vaak besloten in het managementinformatiesysteem (MIS). Gegevens op het hoogste detailniveau voeden algoritmen die leiden tot de bepaling van een stuurgetal of KPI. Bijvoorbeeld individuele ziekmeldingen en aanstellingsgegevens ten behoeve van het bepalen van het percentage ziekteverzuim. Daarmee worden dus persoonsgegevens verwerkt in het MIS. Bovendien bestaat regelmatig de wens – al was het maar voor controledoeleinden ("Waarom is het verzuimpercentage opgelopen naar 3,5%?") – om in te zoomen op detailinformatie. Daarmee worden persoonsgegevens niet alleen door het MIS verwerkt, maar worden deze ook gepresenteerd aan hen die binnen de organisatie toegang hebben tot het MIS. Uiteraard zijn rapportages of dashboards die dergelijke gegevens bevatten goed te autoriseren, maar er is sprake van een privacy-risico.

Ook vanuit het oogpunt van dataminimalisatie en retentieminimalisatie (privacy-by-default) zijn veel managementinformatiesystemen niet in lijn met AVG-eisen. Zo bevatten datawarehouses vaak volledige kopieën van brondatabases. Enerzijds vanuit het oogpunt van minimale belasting van een brondatabase, anderzijds vanuit de gedachte "dan hebben we die informatie maar vast beschikbaar". Vooral die laatste gedachte staat haaks op het doelmatigheids- en integriteitsbeginsel van de AVG.

Bovendien kan de vraag gesteld worden in hoeverre Betrokkenen expliciet toestemming gegeven hebben voor het verwerken van hun persoonsgegevens in een systeem voor managementinformatie. Om bij het voorbeeld van verzuim te blijven, kan gesteld worden dat vanuit rechtmatigheid en doelmatigheid nog te verdedigen is dat op basis van individuele ziekmeldingen een stuurgetal als ziekteverzuimpercentage berekend wordt. Maar wat als diezelfde individuele ziekmeldingen door een manager gebruikt worden bij salarisonderhandelingen? Nog een stap verder worden dergelijke keuzes niet meer gemaakt door een manager maar doen systemen voorstellen voor promotie of demotie van medewerkers op basis van slimme algoritmen. Dat geldt natuurlijk niet alleen voor dit specifieke verzuimvoorbeeld, maar kan bezien worden binnen elk domein: onderwijs, zorg, et cetera.

Kijkend naar de vuistregels van de Autoriteit Persoonsgegevens voor het doen van een risicoanalyse (DPIA) is bij Analytics heel vaak sprake van een privacy-risico uit het oogpunt van de AVG. Het is per definitie grootschalig (punt 3 en 5) en gaat per definitie over het koppelen van databronnen (punt 6). Afhankelijk van de branche (denk Zorg, Onderwijs, Overheid) gaat het vaak over gevoelige gegevens (punt 4) en of kwetsbare personen (punt 7). En tenslotte maken technologische vooruitgang het mogelijk om geautomatiseerde beslissingen te nemen op in MIS opgeslagen data (punten 1, 2, 8 en 9). Analytics staat daarmee per definitie op gespannen voet met de AVG.

Hoe zorg je er toch voor dat je binnen de kaders van AVG toch waarde kunt creëren op basis van data en data-analyse?

AVG-COMPLIANT: EEN VOORTDURENDE INSPANNING

Bij Axians zien we 'AVG-compliant' zijn of worden niet als eenmalige inspanning. Het is een cyclisch proces dat leidt tot blijvende aandacht voor en een continue verbetering in de omgang met persoonsgegevens. Afbeelding 1 geeft deze cyclus weer binnen de kaders van AVG.

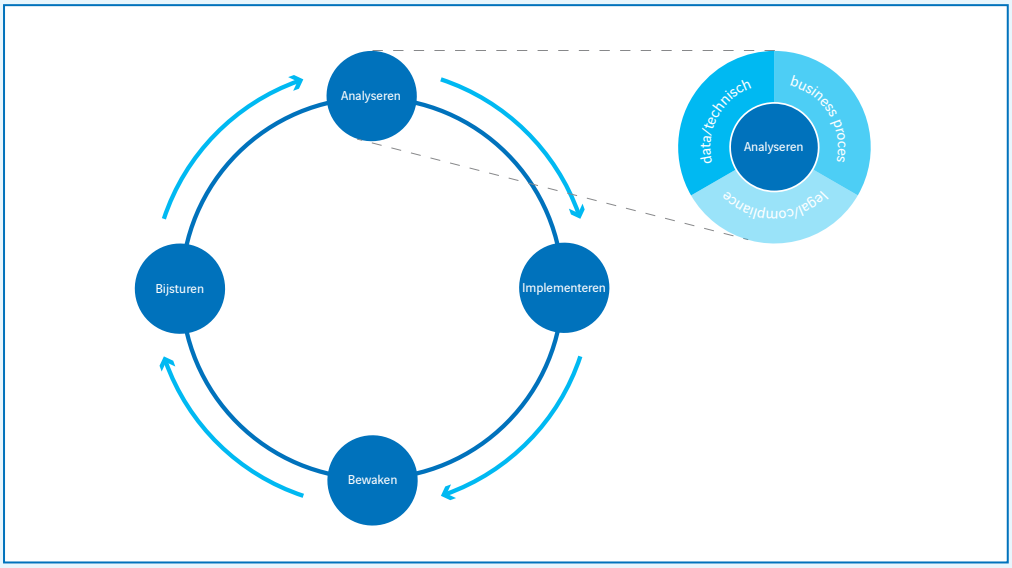
In elke stap van de cyclus onderscheiden we drie focus-gebieden: (1) data/technologie, (2) business processen en (3) legal/compliance. AVG compliancy kan niet slechts binnen één van deze focusgebieden bereikt worden. Bijvoorbeeld: persoonsgegevens in het MIS kunnen goed beveiligd zijn opgeslagen en afdoende geautoriseerd. Dit is echter weinig waard wanneer er geen formeel proces ingericht is waarmee toegang verleend wordt. Wanneer je bovendien niet in staat bent om aan te tonen wie, op welk moment, ook daadwerkelijk gebruikmaakte van zijn of haar toegang tot persoonsgegevens in het MIS, kun je je compliancy niet aantonen (verantwoordingsplicht). Business Analytics specialisten van Axians kunnen je binnen elk van de focusgebieden adviseren of oplossingen bieden die je helpen om op een juiste manier om te gaan met privacygevoelige informatie, bijvoorbeeld met een AVG Assessment.

AVG ASSESSMENT

Tijdens dit assessment beoordelen we in welke mate het MIS van jouw organisatie voldoet aan de eisen van de AVG. Daarbij staan we stil bij alle facetten van het MIS.

Aspecten van het AVG Assessment

- Is er zicht op welke persoonsgegevens in het MIS zijn opgeslagen?
- Hoe stromen persoonsgegevens door het MIS (data lineage)?
- Hoe wordt deze data op fysieke media opgeslagen?
- Zijn persoonsgegevens wel of niet geanonimiseerd?
- Is er een OTAP-straat of een variant daarop? Zijn persoonsgegevens in de Ontwikkel- of Testomgeving wel anoniem?
- Wordt gebruik gemaakt van geavanceerde authenticatiemethoden voor toegang tot het MIS, zoals two-factor authenticatie?
- Hoe is de rollen- en rechtenstructuur van het MIS ingericht?
- Maak je gebruik van auditing tools waarmee je het gebruik van het MIS in beeld kunt brengen?
- Et cetera



Afbeelding 1: AVG compliancy cyclus

Tijdens een AVG Assessment spreken wij met MIS-beheerders, eigenaren en informatiemanagers voor een of meerdere domeinen (bijvoorbeeld Financiën, Personeel en Onderwijs). Op basis van de uitkomsten van het assessment bieden we je concrete oplossingen aan die je helpen te voldoen aan de eisen van AVG. Hierna enkele voorbeelden van producten en diensten waarmee we organisaties helpen.

MODELLERING VAN BEDRIJFSPROCESSEN

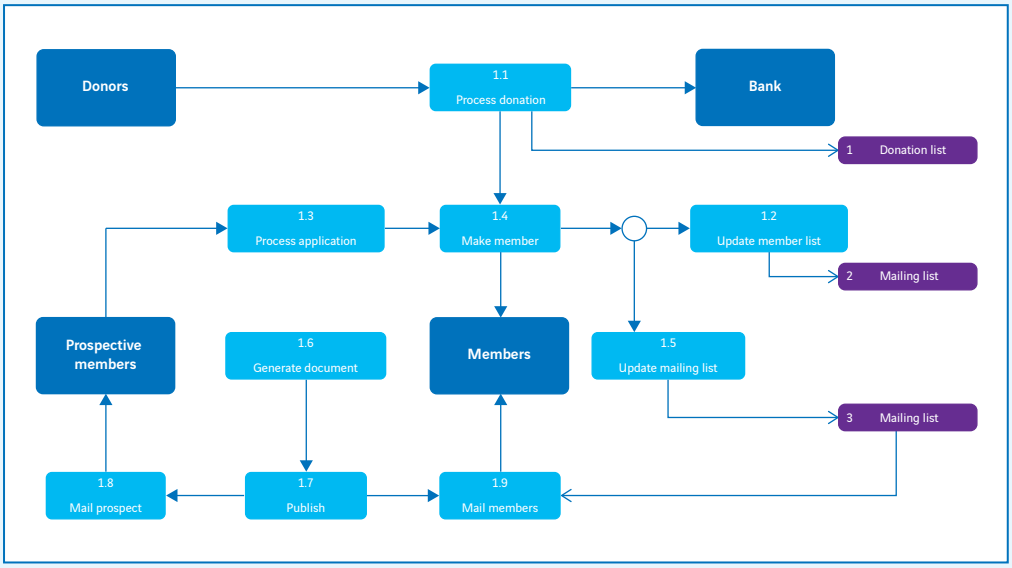
Data, systemen en technologieën waarmee verwerkt wordt, zijn slechts een onderdeel van AVG compliancy. Een ander belangrijk aspect zijn bedrijfsprocessen. Elke organisatie zal tenminste een deel van haar bedrijfsprocessen moeten nalopen - en zeer waarschijnlijk aanpassen - om te voldoen aan door de AVG gestelde kaders. Zelfs als het verwerken van persoonsgegevens niet plaatsvindt ten behoeve van het primaire productieproces. Denk bijvoorbeeld aan de HR-administratie of het CRM-systeem.

Het in kaart brengen en aanpassen van de bedrijfsprocessen kan vergemakkelijkt worden met modelleringssoftware. Dergelijke software stelt je in staat om elk aspect van jouw bedrijfsvoering te modelleren op het detailniveau dat gewenst of vereist is. In het kader van AVG zijn zogenaamde Data Flow Diagrams (DFD) daarbij van groot belang. Stel, je verwerkt bijvoorbeeld data van donaties aan een goed doel. Hoe 'stroomt' de data die daarbij gebruikt wordt door de stichting? In Afbeelding 2 zie je een voorbeeld van zo'n DFD. Op basis van dergelijke DFD's heb je snel inzicht wat er met persoonsgegevens gebeurt en daarmee of deze wellicht gebruikt worden voor doeleinden waarvoor de Betrokkene geen toestemming gaf.

DATA-LINEAGE

Een van de eerste stappen (en misschien wel de belangrijkste) op weg naar AVG compliancy: inzicht in welke persoonsgegevens je verwerkt in het MIS. Uit welke bronnen komen deze? Welke bewerkingen vinden daarop plaats? In welke tabellen van welke database worden deze gegevens opgeslagen? En in welke eindproducten (rapporten, dashboards, kubussen, et cetera) komen deze naar voren.

De tracering van waar (persoons)gegevens vandaan komen en hoe zij – inclusief alle tussenliggende stappen – terechtkomen in verschillende analytics eindproducten wordt data-lineage genoemd. Wij komen veel organisaties tegen waarin slechts een globaal overzicht bestaat van hoe welke (persoons) gegevens verwerkt worden in hun MIS. Vaak ligt dergelijke meta-informatie besloten in verschillende functionele of technische ontwerpdocumenten. Bovendien zijn datamodellen en programmatuur in de loop van de tijd geëvolueerd en zijn de wijzigingen in verwerking niet structureel vastgelegd.



Afbeelding 2: Data Flow Diagram

Veel van de moderne tools waarmee data ontsloten worden (ETL/ELT) bieden de mogelijkheid om in een oogopslag inzichtelijk te maken waar (persoons)gegevens binnen het MIS vandaan komen, hoe deze verwerkt worden, in welke rapporten en dashboards deze getoond worden en zelfs welke gebruikers geautoriseerd zijn om die eindproducten in te zien of te gebruiken. Deze verwerkingsketen kan grafisch weergeven worden, zoals in de afbeelding hieronder. Zo heb je zelf grip op de verwerking van persoonsgegevens en je kunt controlerende instanties eenvoudig inzicht geven.

OTAP-INRICHTING

Het MIS van jouw organisatie bestaat waarschijnlijk niet uit alleen een Productie (P) omgeving, maar je hebt ook een Ontwikkel (O), Test (T) of Acceptatietest (A) omgeving. Bij het inrichten van een OTAP-landschap of variant daarop moet je rekening houden met de eisen die AVG stelt aan verwerking van persoonsgegevens. Zo kan het zijn dat jouw MIS geheel rechtmatig en doelmatig persoonsgegevens bevat. Bijvoorbeeld om studenten op basis van deze data persoonlijk studieadvies te kunnen geven. Of om als Gemeentedienst jouw bedieningsgebied geografisch te analyseren.

Analisten hebben deze persoonsgegevens in de Productie-omgeving tot hun beschikking. Maar ontwikkelaars of technisch testers zouden geen toegang moeten hebben tot deze (niet anonieme) persoonsgegevens. Toch zien we in de praktijk vaak dat ten behoeve van ontwikkel- en testwerkzaamheden een (gedeeltelijke) kopie van data uit de Productie-omgeving gebruikt wordt.

Handig, maar niet toegestaan vanuit de AVG, want niet recht- en doelmatig. Bovendien wordt de kans op een data-lek zo onnodig vergroot. Wij maken gebruik van zowel eigen tooling als tooling van derden om data warehouses ten behoeve van test- en ontwikkelwerk te anonimiseren. Daarbij staat bruikbaarheid van de data voorop. Er moet nog steeds zinnig en adequaat getest kunnen worden.

AUDITING

Controleren en auditeren zijn een essentieel onderdeel in de AVG compliancy cyclus. Als je bedrijfsprocessen in orde zijn en de persoonsgegevens juist worden verwerkt binnen het MIS, dan is de laatste stap het monitoren daarvan. Tools voor datamodellering en data-lineage geven je blijvend inzicht in de logische en fysieke datastromen binnen het MIS, maar meer inzicht is nodig. Bijvoorbeeld in wie op welk moment ook daadwerkelijk gebruikt maakte van persoonsgegevens. En in welke frequentie hij of zij dat deed.

Bij Axians realiseren we analytics oplossingen voor klanten op basis van verschillende tools. Al deze tools houden uitgebreide logbestanden bij van toegang en gebruik. Deze tools bieden bovendien vaak de mogelijkheid om deze meta-data over gebruik (let op: in zichzelf al gevoelige data in relatie tot AVG) gestructureerd uit te lezen. Verscheidene van deze tools hebben op basis van deze metadata standaard dashboards en rapporten beschikbaar. Deze geven je met een druk op de knop de inzichten die je zelf (of auditors) zou willen zien. Daarbij kan het gaan om vragen over wie welke rapporten of dashboards met daarop persoonsgegevens zag. Maar ook om de vraag hoe vaak rapporten met persoonsgegevens ingekeken worden.

Tot slot

Dit whitepaper geeft een globale achtergrond bij de impact van de AVG. De kernboodschap is dat de verwerking van persoonsgegevens belangrijke ontwerpkeuzes met zich meebrengt in processen en systemen; ook in het MIS.

De hierboven genoemde oplossingen zijn een greep uit de dienstverlening die wij onze klanten bieden op het gebied van AVG compliancy. Belangrijk is daarbij dat AVG compliancy niet een eenmalige exercitie is, maar een doorlopend proces van Plan, Do, Check, Act. Wij komen graag met je in gesprek over de AVG in het algemeen en in relatie tot jouw MIS in het bijzonder.

De AVG maakt het op het eerste gezicht lastiger om waarde te creëren uit data. Tegelijkertijd stelt het je voor de opgave om het hoe en waarom van dataverzameling en verwerking in het MIS onder de loep te nemen. Waarom verzamel je deze data en waarom op deze manier? Wij zijn ervan overtuigd dat deze gerichte focus op dit 'waarom' een positieve impuls geeft aan waarde-creatie door data-analyse.

De impact van de AVG is voor elke organisatie anders. Wij helpen je graag om AVG compliant te zijn en te blijven. Neem voor meer informatie of voor het maken van een afspraak contact met ons op via e-mailadres info.bi.nl@axians.com of telefoonnummer (088) 597 55 00.

The best of ICT with a human touch

axians

Eemsgolaan 15
9727 DW Groningen

Esp 120
5633 AA Eindhoven

info.bi.nl@axians.com