axians

DE IMPACT VAN GDPR OP ANALYTICS

WHITEPAPER

GDPR & Analytics

www.axians.nl/business-analytics/gdpr

Axians
Tel: +31 (0)88 597 55 00 - www.axians.nl

VINCI ENERGIES

GDPR & Analytics

Op 25 mei 2018 loopt de zogenaamde 'grace period' voor de *General Data Protection Regulation (GDPR)* af. Op dat moment dient uw organisatie klaar te zijn voor de eisen die deze Europese wet stelt aan de verwerking van persoonsgegevens. De omvang en reikwijdte van deze wet is fors te noemen; niet eerder stelde wetgeving zoveel eisen aan de verwerking van privacygevoelige gegevens.

Wat zijn de implicaties voor uw bedrijfsvoering? Zijn uw processen en systemen 'compliant' ingericht. Veel leveranciers spelen in op dergelijke vragen.

Zoeken op GDPR, of op de Nederlandse term *Algemene Verordening Gegevensbescherming (AVG)*, leidt tot een veelheid aan artikelen in de categorie "Bent u klaar voor GDPR?" of "GDPR komt eraan! Bereid u voor!". Daarin wordt – meer of minder schreeuwerig ("boetes!") – stilgestaan bij de eisen die de wet op hoofdlijnen stelt om vervolgens een scan aan te bevelen om te bezien in welke mate uw organisatie 'GDPR proof' is. Wat veelal mist zijn concrete oplossingen om te voldoen aan de eisen.

Ook, of misschien juist, voor het domein van Analytics geldt dat de GDPR grote gevolgen heeft en wezenlijke aanpassingen aan uw analytics-systemen en -processen verlangt.

Data als grondstof voor de economie

Data wordt gezien als de belangrijkste grondstof van de Economie 4.0. Slim gebruik van data is de weg naar 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 ontvangt, 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 GDPR geïntroduceerd: om een einde te maken aan het ongebreideld verzamelen, opslaan en analyseren van data zonder toestemming of welomschreven doel.

GDPR

De GDPR betreft de *verwerking*, het *beheer* en de *beveiliging* van persoonsgegevens van Europese burgers. De wet gaat uit van een aantal grondbeginselen, waarvan rechtmatigheid, doelmatigheid en integriteit de kern vormen.

Rechtmatigheid gaat over de toestemming voor het verwerken van persoonsgegevens van een persoon. Anders dan nu het geval is moet de betreffende persoon (ofwel de Betrokkene), in de meeste gevallen *expliciet* toestemming geven voor het verwerken van zijn of haar persoonsgegevens of moet deze verwerking 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.

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 of haar persoonsgegevens gebruikt worden. Vage doeleinden – in de trant van "uw gegevens zullen gebruikt worden om onze dienstverlening aan u te optimaliseren" – zijn ontoereikend.

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

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 zolang als nodig voor dat specifieke doel (*retentieminimalisatie*).

Privacy-by-design houdt in aan 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 waarbij geïnventariseerd wordt wat de risico's zijn van het verwerken van persoonsgegevens en welke stappen genomen worden om deze risico's te minimaliseren. Afhankelijk van de omvang van uw organisatie of de aard van dataverwerking kan zo'n DPIA verplicht zijn.

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

1. Beoordelen van mensen op basis van persoonskenmerken
2. Geautomatiseerde beslissingen
3. Stelselmatige en grootschalige monitoring
4. Gevoelige gegevens
5. Grootschalige gegevensverwerkingen
6. Gekoppelde databases
7. Gegevens over kwetsbare personen
8. Gebruik van nieuwe technologieën
9. Blokkering van een recht, dienst of contract

Naast deze grondbeginselen brengt de GDPR een aantal belangrijke wijzigingen ten opzichte van bestaande privacywetgeving met zich mee. Zo worden de maximale boetes bij overtredingen van de

GDPR veel hoger dan nu het geval is (tot 4% van de wereldwijde omzet van de organisatie) en geldt de wet voor alle bedrijven die persoonsgegevens van Europese burgers verwerken, dus ook voor niet in Europa gevestigde organisaties. Datalekken moeten binnen 72 uur gemeld worden. Betrokkenen krijgen het recht om 'vergeten te worden'; zij kunnen een organisatie verzoeken al hun persoonlijke gegevens integraal te verwijderen. Dus ook uit bijvoorbeeld back-ups of een analytics-systeem. Daarnaast hebben zij recht op data-portabiliteit, wat inhoudt dat zij hun gegevens kunnen opvragen ter overdracht aan een derde partij, bijvoorbeeld hun zorg- of leerlingdossier. Tot slot is het in specifieke gevallen – afhankelijk van het type organisatie of de aard en schaal van de gegevensverwerking – verplicht om een Data Protection Officer (DPO) aan te stellen die bewaakt dat verwerking van persoonsgegevens verloopt volgens de GDPR-normen.

Belangrijk is om te realiseren dat u niet alleen verantwoordelijk bent voor het naleven van GDPR in uw eigen organisatie. U dient ook afspraken maken met uw leveranciers en partners over de naleving, onder andere door het afsluiten *verwerkersovereenkomsten*.

GDPR & Analytics

De GDPR is specifiek voor het domein van Analytics een grote uitdaging. Vaak is Analytics binnen organisaties 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 vaak de wens – al was het alleen 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. Natuurlijk zijn rapportages of dashboards die dergelijke informatie bevatten te autoriseren. Vaak is autorisatie in een MIS echter niet automatisch gekoppeld aan autorisaties in het ERP-systemen waaruit data onttrokken zijn. Daarmee vormt het dus een privacy-risico.

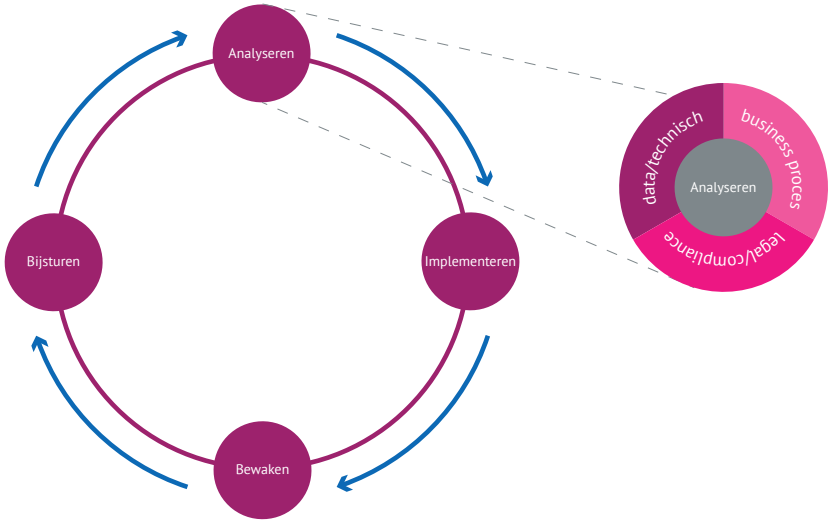
Ook vanuit het oogpunt van dataminimalisatie en retentieminimalisatie (privacy-by-default) zijn veel managementinformatiesystemen niet in lijn met GDPR-eisen. Zo bevatten datawarehouses vaak volledige kopieën van brondatabases. Enerzijds vanuit het oogpunt van minimale belasting van een brondatabase,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

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

GDPR compliant: een voortdurende inspanning

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



Afbeelding 1 GDPR Compliancy Cyclus

In elke stap van de cyclus onderscheiden we drie focusgebieden: (1) data/technologie, (2) business processen en (3) legal/compliance. GDPR compliancy kan niet louter binnen een van deze focusgebieden bereikt worden. Bijvoorbeeld: persoonsgegevens in uw 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 u 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, kunt u uw compliancy niet aantonen (verantwoordingsplicht). Axians Business Intelligence kan u binnen elk van de focusgebieden adviseren of oplossingen bieden die u helpen om op een juiste manier om te gaan met privacygevoelige informatie.

GDPR Assessment

Tijdens dit assessment beoordelen we in welke mate uw MIS voldoet aan de eisen van de GDPR. Daarbij staan we stil bij alle facetten van uw MIS.

Aspecten van het GDPR Assessment.

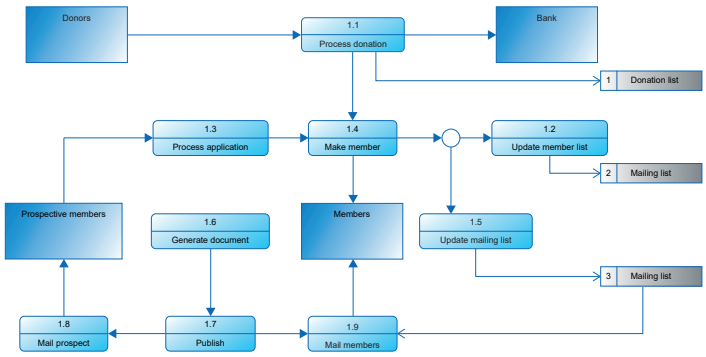
- Hebt u zicht op welke persoonsgegevens u hebt opgeslagen in uw MIS?
- Hoe stromen persoonsgegevens door uw MIS (data lineage)?
- Hoe wordt deze data op fysieke media opgeslagen?
- Zijn persoonsgegevens wel of niet geanonimiseerd?
- Hebt u een OTAP-straat of een variant daarop? Zijn persoonsgegevens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

Tijdens een 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 kunnen we u oplossingen bieden die u helpen te voldoen aan de eisen van GDPR. 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 GDPR compliancy. Een ander belangrijk aspect zijn uw bedrijfsprocessen. Elke organisatie zal tenminste een deel van haar bedrijfsprocessen moeten nalopen en zeer waarschijnlijk aanpassen om te voldoen aan door de GDPR gestelde kaders. Zelfs als het verwerken van persoonsgegevens niet plaatsvindt ten behoeve van uw primaire productieproces. Denk bijvoorbeeld aan uw HR-administratie of uw CRM-systeem.



Afbeelding 2 Data Flow Diagram

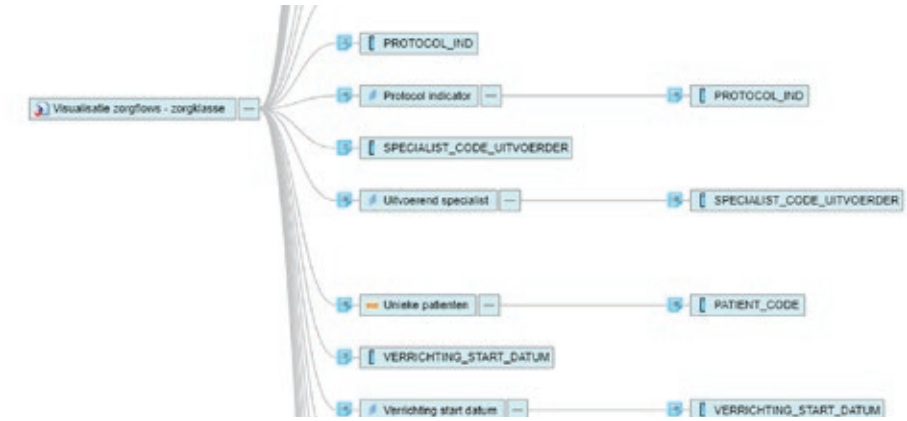
Het in kaart brengen en aanpassen van uw bedrijfsprocessen kan vergemakkelijkt worden door gebruik te maken van modelleringssoftware. Wij maken daarbij gebruik van SAP PowerDesigner. PowerDesigner

stelt u in staat om elk aspect van uw bedrijfsvoering te modelleren op het detailniveau dat gewenst of vereist is. In het kader van GDPR zijn zogenaamde Data Flow Diagrams (DFD) daarbij van groot belang. U verwerkt data, bijvoorbeeld van een donatie aan een goed doel. Hoe 'stroomt' de data die daarbij gebruikt wordt door de stichting? In Afbeelding 2 ziet u een voorbeeld van zo'n DFD.
Op basis van dergelijke DFD's hebt u snel inzicht wat er met persoonsgegevens gebeurt en daarmee of deze wellicht gebruikt worden voor doeleinden waarvoor de Betrokkene geen toestemming gaf.
Daarnaast is PowerDesigner uitermate geschikt voor modelleren van conceptuele, logische en fysieke datamodellen, waarbij u per gegevensveld een categorie kunt koppelen, bijvoorbeeld of het hier een persoonsgegeven betreft.

Data-lineage

Een van de eerste en misschien wel de belangrijkste stap op weg naar GDPR compliancy: inzicht in welke persoonsgegevens u verwerkt in uw MIS. Uit welke bronnen komen deze? Welke bewerkingen vinden er op 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.

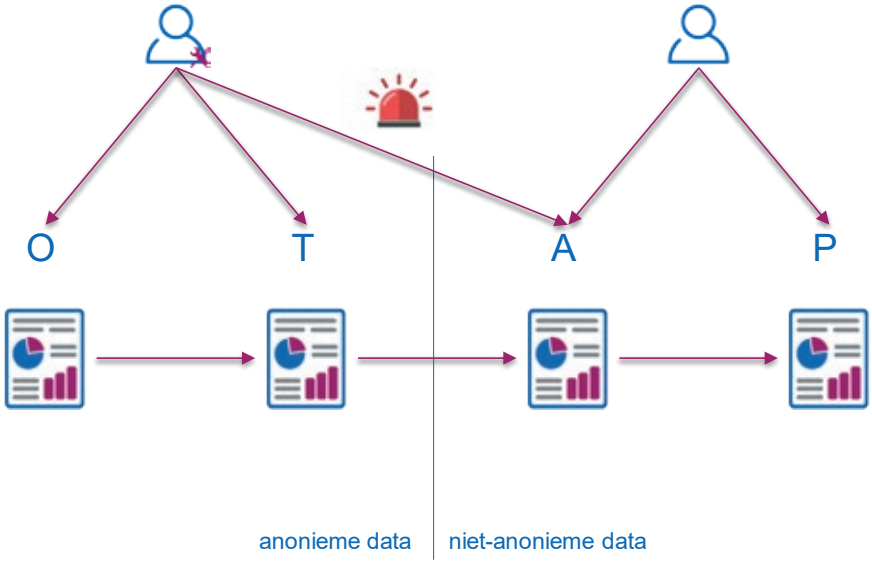


Afbeelding 3 SAP Information Steward

Voor onze SAP BusinessObjects klanten leveren wij SAP Information Steward. Met deze tool maakt u in een oogopslag inzichtelijk 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 wordt grafisch weergeven, zoals in Afbeelding 3 hieronder.
SAP Information Steward maakt deze verwerkingsketen automatisch inzichtelijk op basis van de meta-data in uw SAP BusinessObjects repositories, u hoeft deze ketens zelf niet te modelleren. U hebt zelf grip op de verwerking van persoonsgegevens en u kunt controlerende instanties eenvoudig inzicht geven.

OTAP-inrichting

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



Uw analisten hebben deze persoonsgegevens in de Productieomgeving 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 kopie van data uit de Productie-omgeving gebruikt wordt. Handig, maar niet toegestaan vanuit de GDPR, want niet recht- en doelmatig. Bovendien wordt de kans op een datalek 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 GDPR compliancy cyclus. Uw bedrijfsprocessen zijn in orde en de persoonsgegevens worden juist verwerkt binnen uw MIS; dan is de laatste stap het monitoren daarvan. Tools als SAP PowerDesigner en SAP Information Steward geven u blijvend inzicht in de logische en fysieke datastromen binnen uw 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.

Axians Business Intelligence realiseert oplossingen voor klanten op basis van QlikView/Sense en SAP BusinessObjects. Beide pakketten houden uitgebreide logbestanden bij van toegang en gebruik. Beide

platforms bieden bovendien de mogelijkheid om deze meta-data over gebruik (let op: in zichzelf al gevoelige data in relatie tot GDPR) gestructureerd uit te lezen. Wij hebben op basis van deze meta-data voor zowel Qlik als SAP QuickStart dashboards en rapporten. Deze geven u met een druk op de knop de inzichten die u zelf of die auditors 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 wijzigingen die u kunt verwachten per 25 mei 2018. De kernboodschap is dat u vanaf dat moment een rechtmatige en doelgerichte motivatie nodig hebt om persoonsgegevens te verwerken; ook in uw MIS.

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

Deze nieuwe Europese wetgeving maakt het op het eerste gezicht lastiger om waarde te creëren uit data. Tegelijkertijd stelt het u voor de opgave om het hoe en waarom van dataverzameling en verwerking in uw MIS onder de loep te nemen. Waarom verzamelt u deze data en waarom op deze manier? Wij zijn er echter van overtuigd dat deze gerichte focus op dit waarom een positieve impuls geeft aan waardecreatie op basis van data en data-analyse.

De impact van GDPR is voor elke organisatie anders. Wij komen daarom graag met u in gesprek over de impact voor uw organisatie.

Voor meer informatie, of voor het maken van een afspraak kunt u contact opnemen met Niels van der Kam via e-mailadres info.bi.nl@axians.com of telefoonnummer (088) 597 55 00. Of kijk op www.axians.nl/business-analytics/gdpr

DE IMPACT VAN GDPR OP ANALYTICS

axians

Tel: +31 (0)88 597 55 00 - www.axians.nl

www.axians.nl/business-analytics/gdpr