DATAMODELLERING TOEPASSEN SECURITY EN PRIVACY

Inleiding

In dit whitepaper wordt een toepassingsgebied beschreven voor datamodellering. Een toepassing is een werkveld op het vlak van architectuur of modellering waarbij een aantal data modelleervormen met elkaar gecombineerd worden.

Deze specifieke modelleervormen zijn beschreven in een serie whitepapers. In de whitepapers over toepassingsgebieden gaan we in hoe de verschillende modelleervormen met elkaar gecombineerd worden ter ondersteuning van dit toepassingsgebied

Deze combinatie maakt het vervolgens mogelijk om op adequate wijze een model te communiceren voor dit toepassingsgebied. In een aantal gevallen wordt alleen documentatie geproduceerd, in andere situaties kunnen ook andere zaken geproduceerd worden zoals source code of templates etc.

Doel

Data Security en – Privacy zijn onderdelen van Data Management. Data Security is een werkveld dat binnen elke organisatie waar data wordt verwerkt relevant is. Echter bij de ene organisatie is dit werkveld niet of nauwelijks ontwikkeld terwijl andere organisaties hier een tot in detail gewerkte structuur voor hebben uitgewerkt. Door de komst van nieuwe wetgeving zoals de AVG zal iedere organisatie met dit werkveld te maken krijgen en dient er een inventarisatie gemaakt te worden van risico’s en maatregelen.

Ook privacy kent grote verschillen in volwassenheid bij organisaties. Dit is enerzijds afhankelijk van het soort data dat verwerkt wordt. De ene organisatie werkt veel met privacy gevoelige data, de andere organisatie niet of nauwelijks. Daarnaast is er een afhankelijkheid van wat er met de data gedaan wordt. Zo zullen bijvoorbeeld opsporingsinstanties op een hele andere wijze met privacy om dienen te gaan dan een organisatie in een sector als bouw of facilitair.

Wordt data geproduceerd, verwerkt, opgeslagen en getransporteerd dan zijn security en privacy relevant. Binnen deze activiteiten wordt er data geproduceerd of bewerkt waardoor er inzichten ontstaan die ofwel privacy gevoelig zijn, ofwel de organisatie schade toe kunnen brengen omtrent imago, concurrentie of continuïteit. Rond deze datavergaring dient kennis ontwikkeld te worden over de risico’s die bestaan vanuit privacy en security. Vervolgens wordt gekeken naar welke maatregelen deze risico’s tot een voldoende laag niveau reduceren. Rond al deze aspecten en vragen dient er iemand in de organisatie verantwoordelijk te zijn en dat aspect Vandaar dat hier een nauwe relatie bestaat met Data Governance.

Data modellering en security en privacy lijken in eerste instantie weinig met elkaar gemeen te hebben, echter niets is minder waar. Enerzijds is het tenslotte altijd de data waarin de gevoelige patronen met de bijbehorende risico’s in zijn opgesloten Anderzijds is de waarde en daarmee de risico’s van de data gelegen in de structuur van de data en de mogelijkheid om de structuur naar behoefte te veranderen.

In dit whitepaper behandelen we de Data Security en Privacy voornamelijk vanuit het perspectief van het DaMa International, het consortium achter de DaMa Body of Knowledge, waarbij we regelmatig verwijzen naar achtergrond informatie. De hoofdpagina voor deze site is te vinden via http://dama.org

Context

Data security en privacy managen is voor sommige organisaties een complex en langdurig proces, bij andere organisaties kost dit minder effort. Dit hangt veelal af van de volwassenheid van de organisatie rond security processen. Is men bijvoorbeeld reeds bekend met privacy en security vanwege de aard van de organisatie en zijn reeds processen en rollen ingericht in de organisatie dan is het inregelen van deze processen relatief eenvoudig.

Echter een aantal organisaties is door de komst van de AVG tot het besef gekomen dat in dit werkveld de nodige achterstand bestaat in de eigen organisatie inrichting. Deze organisaties zijn momenteel volop bezig met het inrichten van deze functies. Data modellering kan voor hen een belangrijk hulpmiddel zijn.

Data Security en Privacy zijn een onderdeel van Data Management. Data Management is een aantal aan elkaar gerelateerde bedrijfsprocessen met focus op de diverse aspecten van data. In het DaMa Body of Knowledge wordt het onderstaande raamwerk voor deze bedrijfsprocessen uitgewerkt.

Bron: DMBoK

Vormgeven van security en privacy staat momenteel bij iedere organisatie op de agenda. Dat is verklaarbaar. Dataverwerking wordt steeds complexer, de waarde van data in de organisatie wordt steeds meer onderkend. Daarnaast neemt de hoeveelheid data waarmee organisaties werken meer en meer toe en ontstaan er big data toepassingen. Als laatste is de noodzaak van compliancy ten aanzien van nieuwe (Europese) wet- en regelgeving een belangrijke reden om data security en privacy naar een hoger niveau te brengen.

DOELEN VAN DATA SECURITY EN PRIVACY

Reden van data security en privacy zijn met name gericht op het inventariseren van de risico's en het nemen (en bewaken) van risico verminderde maatregelen rond de data. In dit whitepaper lichten we een aantal doelen toe van data security indien ze relevant zijn voor data modellering

- **Stakeholders**, vanuit dit perspectief is er behoefte aan maatregelen rond privacy gevoeligheid van data, gevoeligheden rond concurrentie en andere handelsbelangen (overnames etc).
- **Overheid en wetgever,** bepalen regelgeving rond de toegang tot data, registratie van security maatregelen en andere compliancy.
- **Business belangen,** denk hierbij aan handelsbelangen, research en productontwikkeling, overnames en andere zaken op bedrijfseconomisch vlak.
- **Toegang,** toegang tot data dient adequaat geregeld te zijn, maar ook toegang tot gebouwen, bijzondere bedrijfsonderdelen etc. Daarnaast dienen de maatregelen het werken met data voor de betrokken medewerkers niet beperkend te werken.

SECURITY EN DATA MODELLERING

Security en privacy en met name het inventariseren van risico's en maatregelen kan op eenvoudige wijze met data modellering worden uitgewerkt. Door dit te combineren met een aantal andere datamodelleerwijzen ontstaat een aantal weergaven cq viewpoints op de data die de inventarisatie kan vereenvoudigen èn in verband kan brengen met andere zaken zoals data governance en data modellering.

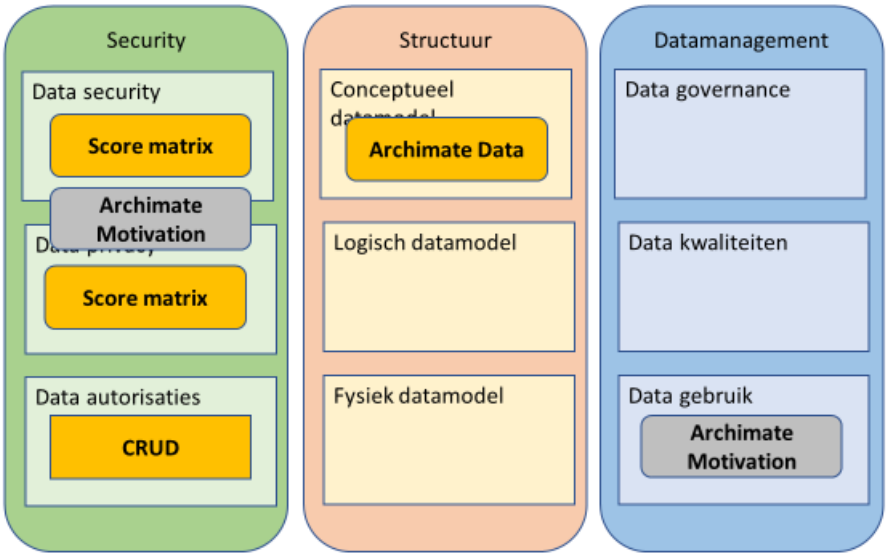
Binnen informatiebeveiliging en privacy wordt veelal een indeling gebruik bestaande uit vier categorieën:

- **Beschikbaarheid**: beschikbaarheid van de data ter ondersteuning van de werkprocessen die gebruikmaken van de datasets die noodzakelijk zijn voor het nemen van beslissingen binnen deze processen.
- **Integriteit**, is een samenvoeging van een aantal datakwaliteiten (zoals uitgewerkt in het toepassingsgebied data quality) die zorgdragen voor de verschillende dimensies van integriteit zoals compleetheid, correctheid en actualiteit.
- **Vertrouwelijkheid,** risico's en maatregelen die noodzakelijk zijn om te zorgdragen dat de inhoud van de data niet gebruikt wordt door personen cq werkprocessen die daartoe niet gerechtigd zijn.
- **Privacy,** een extra categorie en verbijzondering van de andere drie categorieën die zorgdraagt voor de bescherming van de privacy van diverse stakeholders.

Deze vier categorieën worden gebruikt als indeling van inventarisaties en maatregelen.

Notatiewijzen

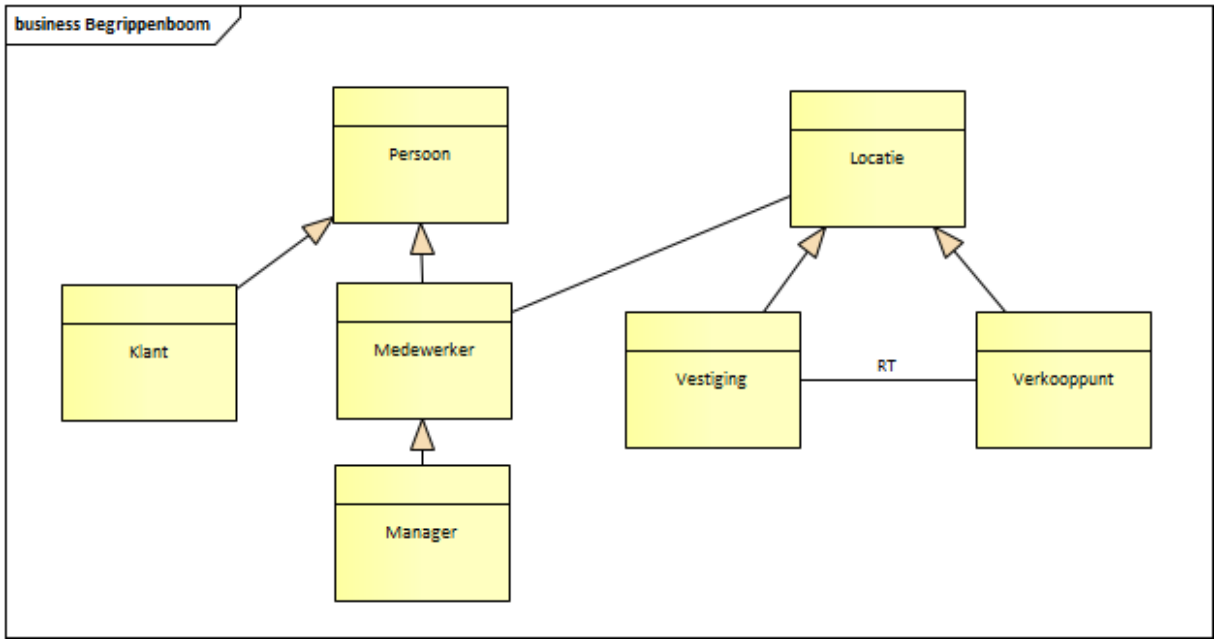
Voor data modellering binnen data security en privacy zijn een aantal notatiewijzen relevant. Een aantal is essentieel, en een aantal is ondersteunend. Onderstaande afbeelding geeft een beeld van de notatiewijzen die vervolgens kort worden toegelicht



CONCEPTUEEL DATAMODEL

Het conceptueel datamodel is voor security en privacy een essentieel onderdeel dat zorgt voor de beschrijving welke data entiteiten cq data sets relevant zijn binnen de organisatie en waarvoor een BIVP classificatie opgesteld dient te worden. Dit is input voor het definiëren welke risico's en maatregelen er een rol spelen bij de bovengenoemde datasets.

Onderstaande afbeelding geeft een beeld van een eenvoudig conceptueel datamodel uitgewerkt binnen de ArchiMate notatie. Meer informatie over de notatiewijze is te vinden via: http://assistent.interactory.nl/cmsForm.aspx?formid=50027&webcontentid=248

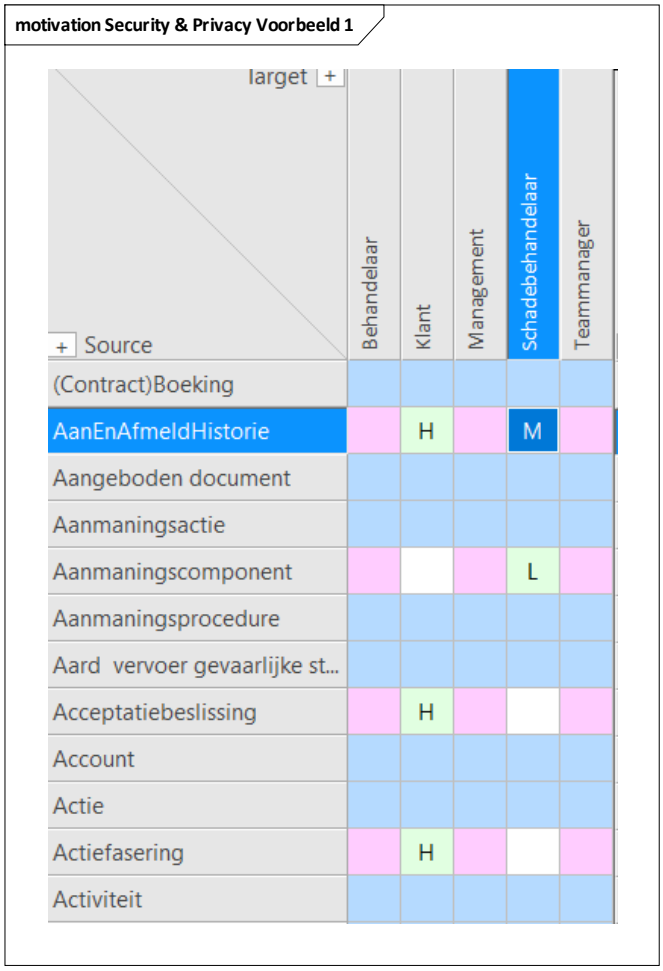


DATA PRIVACY & SECURITY

Voor het modelleren van de security en privacy wordt zoals reeds aangegeven gebruik gemaakt van een viertal categorieën waarbij er op basis van een score een indeling gemaakt worden in hoeverre bepaalde risico's een rol spelen bij een dataset.

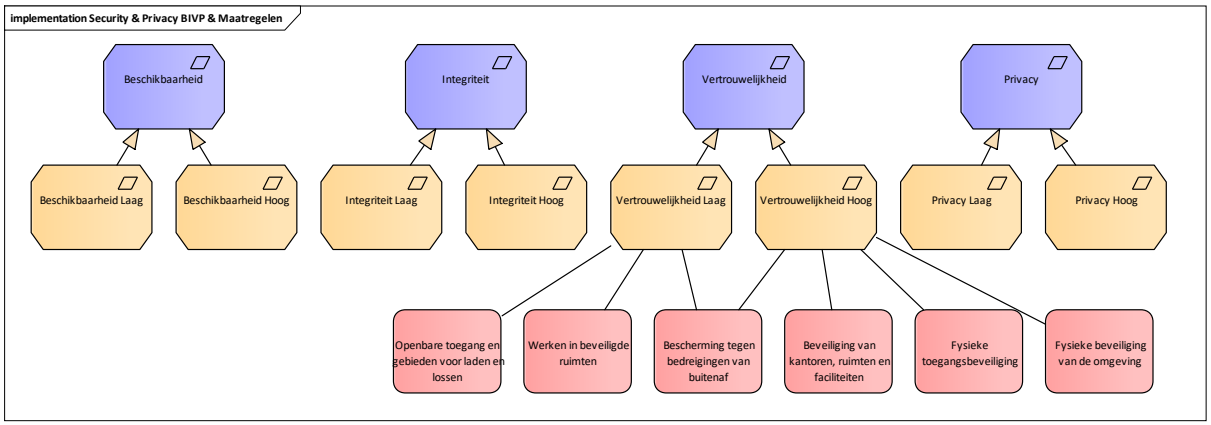
Dit wordt veelal gedaan door een checklist in te zetten en deze te gebruiken voor het bepalen van de hoogte van de risico's. Hiervoor is een scorematrix een goed hulpmiddel. Deze geeft per BIVP categorie en datasets aan wat de hoogte van het risico is. Dit kan met een numerieke score tussen 0 en 10 mogelijk. Echter veelal volstaat een Laag-Midden-Hoog indeling. Zie voor meer informatie het whitepaper:

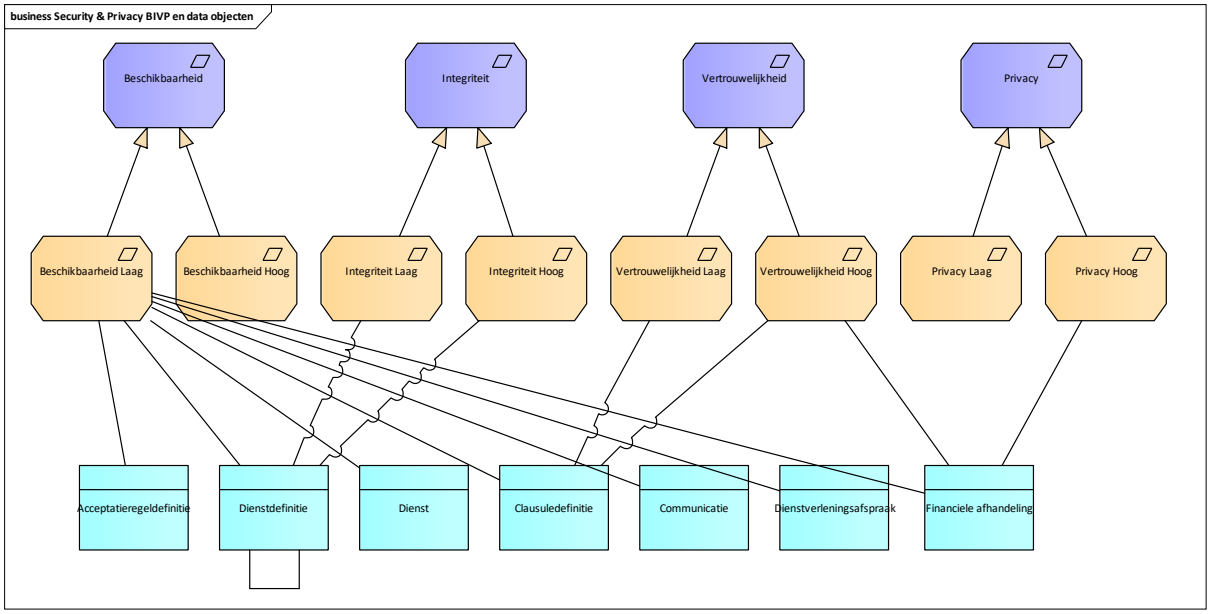
http://assistent.interactory.nl/cmsForm.aspx?formid=50027&webcontentid=256



Op basis van deze risico inventarisatie is het mogelijk te bepalen welke maatregelen noodzakelijk zijn om deze risico's op voldoende wijze af te dekken. Hiervoor kun je op eenvoudige wijze een model opstellen van requirements en de te nemen maatregelen om op visuele wijze de verbanden in beeld te brengen.

De ArchiMate motivation kan hierbij ingezet worden in combinatie met de data entiteiten en eventueel workpackages om maatregelen vorm te geven. Zie hiervoor het whitepaper: http://assistent.interactory.nl/cmsForm.aspx?formid=50027&webcontentid=247



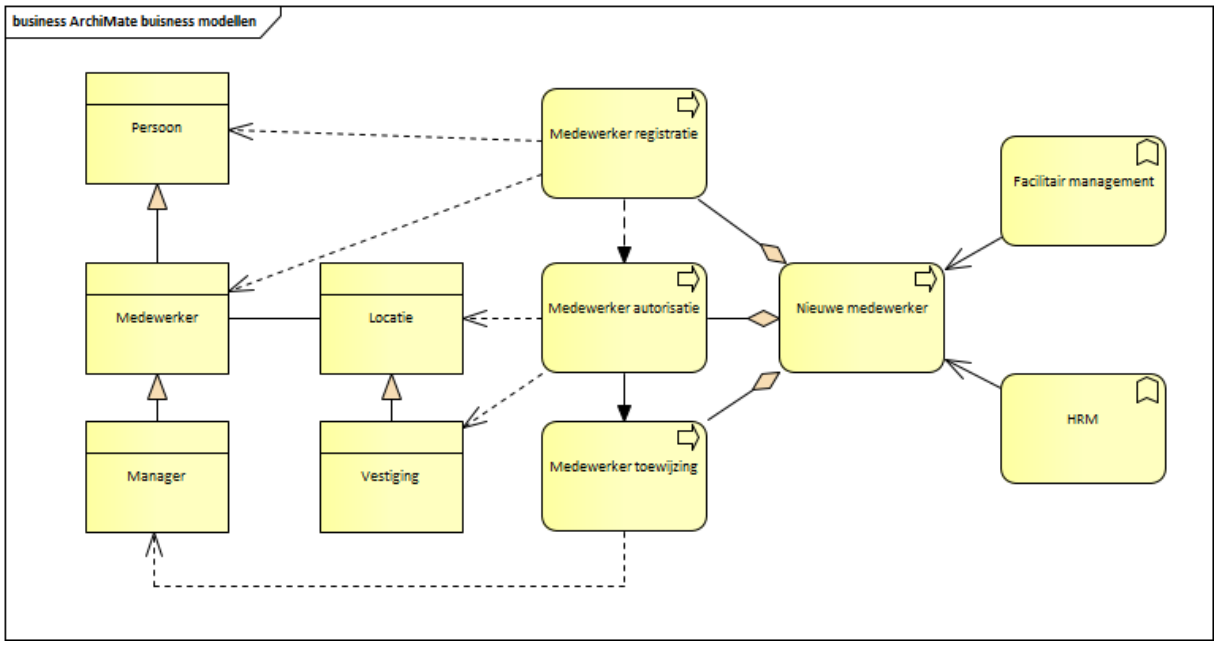


DATA GEBRUIK

Voor informatiebeveiliging en privacy activiteiten is het handig als er inzage is waar de datasets in de organisatie worden ingezet. Dat is niet noodzakelijk maar zeker bij een complex landschap of een hoge volwassenheid van de organisatie rond data management zal hieraan steeds meer behoefte ontstaan.

Data gebruik kan op meerdere niveaus gemodelleerd worden, bijvoorbeeld door in kaart te brengen in welke bedrijfsprocessen een data entiteit gebruikt wordt of door te modelleren in welke applicaties een data entiteit gebruikt cq gemuteerd wordt. Onderstaande afbeelding geeft een voorbeeld van een koppeling tussen de bedrijfsprocessen en de entiteiten. Meer informatie over beide notatiewijzen is te vinden via:

http://assistent.interactory.nl/cmsForm.aspx?formid=50027&webcontentid=244 en
http://assistent.interactory.nl/cmsForm.aspx?formid=50027&webcontentid=246



Data autorisaties

Een onderdeel van maatregelen rond privacy en informatiebeveiliging is dat de organisatie zorgdraagt voor de autorisaties van bedrijfsrollen in relatie tot de datasets. Op adequate wijze de juiste toagangsrechten tot data inregelen binnen organisaties is een complex proces met veel dimensies. Het uitwerken van een data model dat de autorisaties inzichtelijk maakt kan hierbij een goed hulpmiddel zijn.

Hiervoor is een CRUD matrix een goed hulpmiddel. Een CRUD matrix geeft aan per dataset welke bedrijfsrol, lees, creer, muteer en verwijder rechten heeft. Meer informatie over de CRUD matrix is te vinden in whitepaper: http://assistent.interactory.nl/cmsForm.aspx?formid=50027&webcontentid=250

Onderstaande afbeelding is een voorbeeld van een eenvoudige CRUD matrix:

Target / Source	Manager	Medewerker	Salarisadministratie
Manager	CR		CR
Medewerker	CRUD	CRUD	
Uur	CRUD	CRUD	R
Vestiging	CRUD	CRUD	

Kenmerken

Informatiebeveiliging en privacy komt bij steeds meer organisaties hoger op de prioriteitenlijst te staan. Met name door de introductie van de AVG en de compliancy die daarbij hoort. Daarnaast neemt de hoeveelheid data die door organisaties verwerkt worden verder toe wat aanvullende eisen brengt rond informatiebeveiliging. Maar ook de mogelijkheid om waarde te creëren uit data is een reden om een aantal maatregelen op het gebied van informatiebeveiliging te introduceren.

Security en privacy bieden vanuit data modelleringsperspectief een aantal interessante modelleerbehoeften, met name de combinatie van de verschillende matrices op het vlak van BIVP classificatie in combinatie met het conceptuele model is de kern in een security datamodel. Bij de introductie van data modellering van een security en privacy model zijn de volgende kenmerken relevant:

- Neem BIVP classificaties als uitgangspunt en werk op basis van deze score modellen een aantal maatregelen uit
- Leg een Score matrix aan voor de BIVP classificatie
- Werk eventueel met ArchiMate modellen voor de requirements en de maatregelen
- Voeg detail toe door CRUD matrices op te stellen of door privacy maatregelen op attribuut niveau uit te werken (indien relevant)
- Verfijn het model en breidt het verder iteratief uit.

Producten

De producten voor een data security en privacy vanuit data modelleringsperspectief zijn samengevat:

- Conceptueel datamodel
- Score Matrix obv BIVP
- Modellen rond requirements en maatregelen
- CRUD matrix

Tooling

Zoals reeds genoemd zijn er rond data security meerdere producten te vinden, veelal als onderdeel van een data management suite. Er zijn meerdere specifieke producten zoals bijvoorbeeld Privacy Perfect

Ook generieke tooling kan ingezet worden. Inrichten op basis van Wiki's is een goede mogelijkheid, maak bij de inrichting van een dergelijke omgeving direct rekening met het beheer van de entiteiten. Een dergelijke omgeving dient namelijk in sync te blijven lopen met de ontwikkelingen binnen de data beveiliging inrichting en dat is geen eenvoudige opgave vanuit beheerperspectief.

Als laatste is het inzetten van generieke (enterprise) architectuurtooling te noemen. Een aantal architectuur tools hebben de mogelijkheid om meerdere modelleertalen met elkaar te combineren waardoor de (data) modelleerbehoefte voor data security grotendeels kan worden afgedekt.

Evaluatie

Data security en privacy wordt bij steeds organisaties een belangrijk werkveld. Inzetten van data security kan veel redenen hebben, echter vrijwel altijd is compliancy aan de AVG één van de redenen.

Binnen data security speelt data modellering een steeds belangrijker rol. Met name het leggen van verbanden tussen de data entiteiten en de BIVP classificatie is essentieel. In een vroeg stadium nadenken welke modelleervormen relevant zijn, hoe deze aan elkaar verbonden worden en hoe de stakeholders daarbij betrokken zijn ondersteunt de introductie van adequaat informatiebeveiligingsbeleid.

In dit whitepaper hebben we een combinatie van modelleervormen beschreven die een (minimale) set is van notatiewijzen op basis waarvan data security en -privacy in organisaties gemodelleerd kunnen worden.

Over de auteur

Bert Dingemans is trainer op het vlak van data architectuur, data management en Big Data. Hij heeft een passie voor modelleren, modelleertools en het effectief inzetten van geautomatiseerde hulpmiddelen om modellen effectief in te zetten in de praktijk. Bert is te bereiken via bert@interactory.nl