Duthler Associates
law, ICT & organisation

White paper

De wisselwerking tussen de Europese AVG en de Digitale Transformatie

Over Duthler Associates

Duthler Associates (1998) geeft bedrijven en instellingen advies, doet onderzoeken en voert projecten uit op het vlak van juridische functie, beschermen van persoonsgegevens, informatieveiligheid en informatiebeheer, digitale transformatie en governance & compliance.

Aanleiding

De Europese Algemene verordening gegevensbescherming (Avg) is vanaf 25 mei 2018 van kracht en wordt gehandhaafd. De samenhang tussen de impact van de Avg en de voordelen als gevolg van de digitale transformatie zijn opmerkelijk. Zowel het voldoen aan de Avg als het uitvoeren van een digitale transformatie zijn noodzakelijk voor de bedrijfscontinuïteit.

Het gaat om de wisselwerking tussen Avg en de digitale transformatie. We lichten in deze paper de maatregelen toe die een antwoord zijn op de gevolgen van de wisselwerking tussen Avg en de digitale transformatie voor de bedrijfsvoering. Een organisatie moet in staat gesteld worden om op een effectieve en kostenefficiënte wijze aan het maatschappelijk verkeer deel te nemen. In termen van de Europese toezichthouder gaat het om "*accountable*" te zijn.

En: Duthler Academy heeft een module[1] hierover ontwikkeld.

Observaties

Er bestaat geen eenduidige definitie van de digitale transformatie. Elke organisatie vult het begrip anders in. Daarom beperken wij ons tot de doelstelling die primair van belang is: *dat is dat het bedrijfsproces ongestoord verder kan gaan. De organisatie vervult een aantal kritieke processen en functies die niet onderbroken kunnen worden.*

Daarnaast gaat het ook over het verminderen van de operationele kosten van IT. Als gevolg van het goed uitvoeren van het Avg en DT traject ontstaat een meer productieve en efficiënte bedrijfsvoering. We kunnen daaraan toevoegen het verlagen van het risicoprofiel van de organisatie voor bijvoorbeeld cybersecurity en beheer, en het terugdringen van de bezorgdheid voor het instandhouden van de operationele organisatie. Helaas zien wij in de praktijk vaak dat trajecten rond digitale transformatie niet altijd leiden tot de gewenste resultaten.

Hoe verloopt een dergelijk traject?

Het start dikwijls met het ontwikkelen van digitale CRM gerelateerde applicaties, "*shiny objects*" die gekoppeld worden aan de bestaande IT legacy omgeving. Vervolgens wordt uit efficiencyoverwegingen de bestaande omgeving naar de cloud gebracht, waarbij men veelal start

[1] Meer informatie zie: https://www.duthleracademy.nl/modules/pe-module-digital-transformation/

met de kantoorautomatisering. Het gaat hierbij om het netwerk en de officeproducten. Daarna worden stappen gezet om de financiële en salarisadministratie naar de cloud over te brengen. Met het nodige geluk wordt het traject van het onderbrengen van identificatie, authenticatie en autorisatiemanagement in de cloud succesvol afgerond. Het resultaat is dat applicaties met de samenhangende bedrijfs- en persoonsgegevens naar een gerespecteerd platform zijn gebracht. In de praktijk blijkt echter dat men de heterogene applicatieomgeving één op één overzet naar een hybride of multi-cloud omgeving.

Lift & Shift

Als de bovenstaande stappen gezet zijn is er geen sprake van digitale transformatie omdat data integratie (een corporate datamodel) niet heeft plaatsgevonden. De applicaties staan nog steeds (off-premise) centraal en de bedrijfs- en persoonsgegevens zijn versnipperd in de databases van de applicaties vastgelegd (we spreken hier liever over "opgesloten"). Feitelijk heeft een één op één overgang plaatsgevonden: "*lift & shift*" van eigen of gehuurde infrastructuur naar een gesourced platform. Wij noemen dat ook wel het "*ver-saas-en*" van applicaties of outsourcen. Er is geen sprake van digitale transformatie. De beoogde resultaten van een meer effectievere organisatie en het substantieel verlagen van de operationele kosten alsmede de verschuiving plaats laten vinden van vaste naar variabele kosten blijven veelal uit. Sterker nog, de operationele kosten van de gehele organisatie lopen exponentieel op omdat de legacy systemen aangevuld met nieuwe gedigitaliseerde bedrijfsprocessen de complexiteit verhogen en inefficiënter maken.

Bepalen van de juiste doelstellingen

Het vraagt om een meer structurele benadering om te kunnen spreken van digitale transformatie. Om te beginnen moet worden nagegaan welke doelstellingen van de organisatie door welke bedrijfssystemen worden ondersteund. En vervolgens of dit effectief en efficiënt plaatsvindt. Bij het beoordelen hiervan komt de vraag op tafel of de doelstellingen aansluiten bij de verwachtingen van de klanten. Wellicht zijn er fundamentele aanpassingen nodig in de dienstverlening en / of moeten de bedieningsconcepten opnieuw worden doordacht. Technische ontwikkelingen moet je verkennen om na te gaan of je effectiever en efficiënter kan werken met als doel de burger beter te bedienen. Het gaat erom de vraag te beantwoorden: kan de huidige operationele organisatie de toegevoegde waarde leveren? In de praktijk blijkt dat 85% van alle bedrijfsprocessen en dito applicaties geen waarde toevoegen en niet onderscheidend zijn. Door de niet authentieke applicaties te "ver-saas-en" en te koppelen aan nieuwe digitale functies wordt de latency van de infrastructuur onder druk gezet. Dit leidt onvermijdelijk tot een verslechterde financiële performance en vervroegde afschrijvingen wegens "*under performance*".

Valkuilen van digitale transformatie

Digitale transformatie (DT) klinkt gemakkelijk maar de ervaring leert dat het flink kan tegenvallen. Een niet goed doordachte migratie zoals hierboven beschreven, maar overigens wel gangbaar in de markt, veroorzaakt grote financiële risico's. DT raakt alle onderdelen van de organisatie en het doorvoeren van een DT traject kent vele culturele en sociologische vraagstukken voor burgers en medewerkers. Het vraagt van de organisatie vindingrijkheid, veerkracht en veranderingsvaardigheid. Het management moet in staat zijn iteratief strategische keuzes, sturingsparadigma's, operationele processen en IT te overzien. Het kan betekenen dat afscheid moet worden genomen van langlopende bedrijfsprocessen waarop de dienstverlening van de organisatie is gebouwd ten behoeve van nieuwe bedrijfsprocessen die hun waarde nog moeten bewijzen. Het vraagt van het management moed om dergelijke stappen te zetten.

Digitale transformatie? Waarom?

Bij het afwegen door het management van het al dan niet uitvoeren van een digitale transformatie traject staan aan de ene kant de zekerheid van de lopende operationele processen en aan de andere kant existentiële argumenten. Waarom zou een organisatie een dergelijk traject opstarten en vervolgens uitvoeren?

Volgens ons is het enige juiste antwoord: *een organisatie moet een digitaal transformatie traject ingaan om de continuïteit van de bedrijfsvoering veilig te kunnen stellen.*

Bedrijven en instellingen hebben echter geen intrinsieke motivatie voor het uitvoeren van een dergelijk traject. De motivatie bij het management komt voort uit signalen van de omgeving en de IT-afdeling vanwege het toepassen van verouderde technologie. Maar als het management dan toch besluit er geen aandacht aan te geven dan zijn de onderstaande argumenten van toepassing om juist wel aandacht te geven aan digitale transformatie.

Elementen van een dergelijk traject

Hoe ziet een dergelijk traject er dan uit? In het algemeen komen de volgende elementen steeds terug:

1. Het is onvermijdbaar. Volgens Forrester Research zullen steeds meer diensten/ services digitaal zijn;
2. De bedrijven die digitale transformatie trajecten hebben doorlopen bevestigen dat er daardoor minder risico is op onderbreking;
3. Na het doorlopen van een succesvol digitale transformatie trajecten zijn de operationele processen van organisaties meer "*lean and mean*" en daardoor effectiever en efficiënter;
4. De operationele organisatie moet flexibel, effectief en efficiënt zijn. Het gaat er om dat snel goed wordt ingespeeld op ontwikkelingen in de omgeving en bovenal op vragen en behoefte van de burgers;
5. Het management schept een cultuur en laat een leiderschap zien die aansluiten bij het centraal zetten van de vragen en behoeften van de burgers. Zoals al eerder gezegd is digitale transformatie een cultureel en sociologische vraagstuk.

Op basis van bovenstaande elementen kan de strategie worden uitgewerkt. Bij het formuleren van een strategie kan gebruik worden gemaakt van vele voorbeelden van digitale transformatie frameworks. Wij hebben inmiddels kennis gemaakt met de frameworks MIT Sloan, Cognizant, Altimeter en Ionology. Het is slechts een deel van mogelijke frameworks. Succesvolle ervaringen met het uitvoeren van digitale transformatie trajecten zijn beperkt. Het begeleiden vergt een multidisciplinair team.

Met de Europese Avg zijn er nieuwe doorslaggevende argumenten ontstaan voor het starten van een digitaal transformatie traject. Wij vervolgen de observaties vanuit het perspectief van de Avg en leggen relaties met digitale transformatie.

ANALYSE VAN DE ZORGSECTOR ALS VOORBEELD

Een recent artikel laat zien dat het zorgdomein nog niet op het gewenste niveau van dataportabiliteit is aangekomen en dat er een enorme inspanning van de sector gevraagd wordt. Alle zorgaanbieders en zorgprofessionals zullen semantisch inter-operabele gegevens en gegevensuitwisseling centraal moeten zetten om te voldoen aan de rechten van de patiënt.

Dit vereist dat de bedrijfs-centrische gegevensverwerking van persoonsgegevens omgezet wordt naar een patiënt-centrische, of nog beter individu-centrische gegevensverwerking. Zorgaanbieders en zorgprofessionals kunnen dit alleen realiseren als de applicatie-centrische informatie-architectuur wordt omgezet naar een data-centrische informatie-architectuur. Je zou kunnen

zeggen dat de zorgaanbieders en zorgprofessionals een digitale transformatie traject nodig hebben om te kunnen voorzien in de rechten van de patiënt.

Met het van kracht worden van de Avg en aanpalende wetweging heeft de betrokkene rechten gekregen die eenvoudig en tegen lage kosten uitgeoefend kunnen worden. Dit zet veel tijdsdruk op bedrijven en instellingen om dat te kunnen faciliteren.

"Avg zet veel tijdsdruk op bedrijven en instellingen om de rechten van de betrokkenen te kunnen faciliteren."

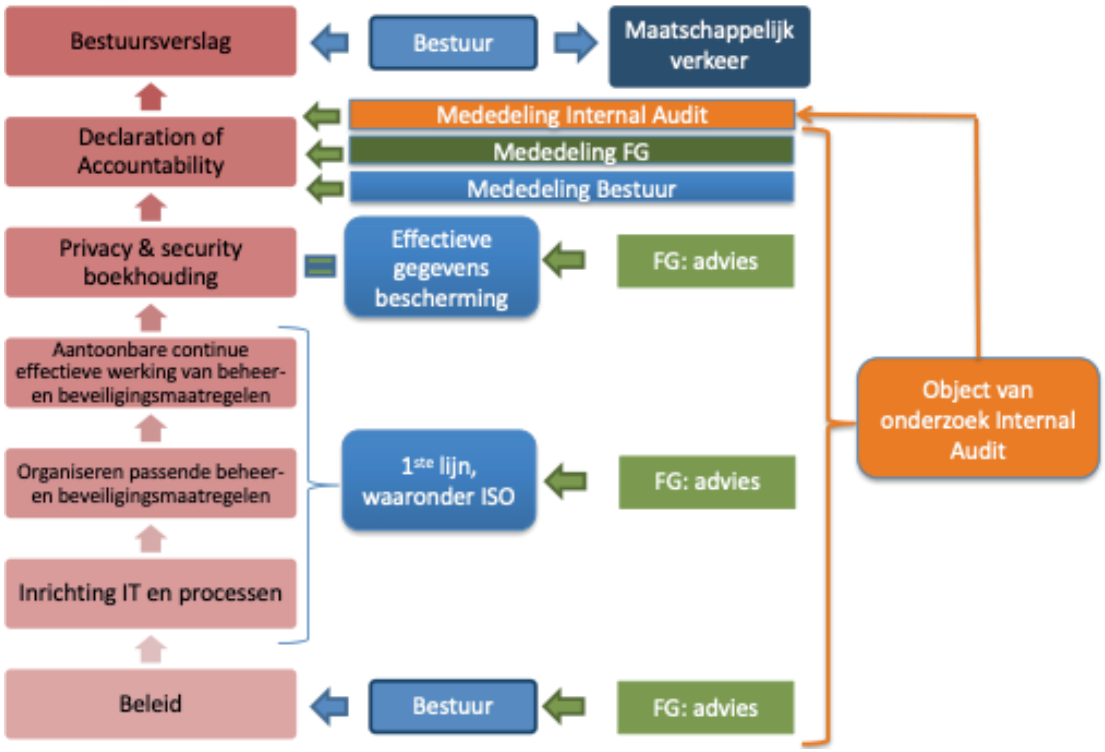
Het doorlopen van een digitale transformatie traject, waarbij rekening wordt gehouden met wet- en regelgeving, ligt voor organisaties niet voor de hand. Maar een traject rond digitale transformatie zonder rekening te houden met de eisen vanuit de Avg is moeizaam en andersom ook.

VRAAG OM OVERHEIDSBEMOEIENIS

In een recent NOS-artikel wordt door ChipSoft gevraagd om overheidsbemoeienis. Wij nemen aan dat de vraag gaat over de regiefunctie gericht op een semantische inter-operabel zorg-ecosysteem. De gewenst geachte overheidsbemoeienis stopt echter niet bij de landsgrenzen. Het gaat immers over de Europese Avg. Hoewel de meeste (persoons-) gegevens vooral regionaal worden uitgewisseld, kan het gebied van de regio tot over onze landsgrenzen reiken. Het vraagt niet veel verbeeldingskracht om te zien dat er regionale informatie ecosystemen ontstaan die onderling inter-operabel zijn en waarbinnen (persoons-) gegevens worden verwerkt.

Nu wij het perspectief van de betrokkene hebben geduid nemen wij de vereiste *accountability*, de verantwoordingsplicht en de rol van de leiding van de organisatie, de functionaris voor gegevensbescherming (FG) en interne controle gericht op compliance in ogenschouw.

Binnen de gebruikelijke governance & compliance cyclus (afbeelding 1, hierboven) kunnen wij de *accountability* van de leiding voor het beschermen van persoonsgegevens van betrokkene in overeenstemming met de wet vormgeven. Hieronder geven dit schematisch weer.



Afbeelding 1 Governance & Compliance Cyclus

De leiding formuleert beleid en de FG adviseert. Vervolgens zorgt de leiding dat het beleid wordt uitgevoerd en uiteindelijk wordt verantwoord in het bestuurdersverslag. Vervolgens begint de governance & compliance cyclus weer opnieuw.

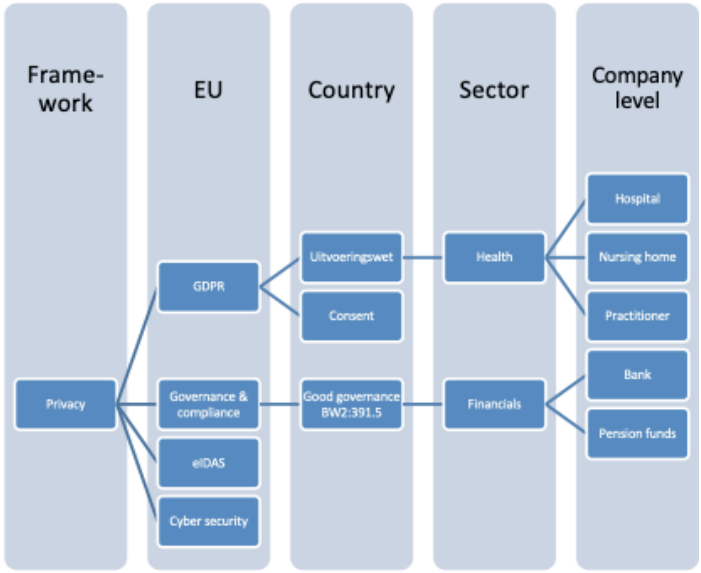
De verantwoordingsplicht vraagt van de leiding zich uit te spreken over de effectieve werking van de getroffen beheers- en beveiligingsmaatregelen gericht op het beschermen van de persoonsgegevens zoals bepaald door de Avg en aanpalende wet- en regelgeving.

De leiding en de FG wordt comfort geboden als een intern controlemechanisme is ingesteld. Wij hebben dat in het bovenstaande model aangegeven als het bevestigen van de *Declaration of Accountability* (het verslag van verantwoording).

In de opbouw van de verantwoordingssystematiek van beleid naar bestuur verslag veronderstellen wij een vertaling van beleid in "Inrichting IT en processen", "Organiseren van passende beheer- en beveiligingsmaatregelen" en accounting op "Aantoonbare continue effectieve werking van beheers- en beveiligingsmaatregelen". Dat vraagt de wetgever van de verwerkingsverantwoordelijke alsmede de verwerkers en sub-verwerkers waarmee de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

Laws and regulations:

- EU law:
  - General Data Protection Regulation (GDPR);
  - eIDAS Directive
- General laws such as:
  - Civil Code;
  - Public Law Act;
  - Criminal Law;
- Sectoral laws:
  - Medical treatment agreement law;
  - Financial Supervision Act;



Afbeelding 2 Relevante wetten en regels

Een uitgangspunt van beleid is compliant zijn aan het wettelijk kader en over de compliance verantwoording afleggen. In het overzicht hierboven (afbeelding 2) worden relevante wetten en regels in verband gebracht en beleidskaders afgeleid. In het bovenstaande overzicht worden voor drie beleidskaders geformuleerd die steeds actueel gehouden moeten worden voor jurisprudentie of voor nieuwe wet- en regelgeving.

De beleidskaders of policy vormen ankerpunten voor het formuleren van normenkaders of baselines die vervolgens toegepast worden in organisaties. Een voor de hand liggende structuur zou kunnen zijn:

- Strategisch niveau (het beleid). Op dit niveau bepaalt de leiding en neemt besluiten. In het bestek van deze paper wordt het (privacy- en veiligheid) beleid hier vastgesteld en wordt verantwoording afgelegd aan het maatschappelijk verkeer;
- Interne controle of bedrijfsbureau (Aantoonbare continue effectieve werking van beheer- en beveiligingsmaatregelen). Op dit niveau wordt de interne sturing van de organisatie uitgevoerd. Wij kunnen denken aan planning & controle, administratie en HR. Voor grote bedrijven en instellingen zullen het omvangrijke afdelingen zijn. Voor een artsenpraktijk blijft het vaak beperkt tot een secretaris;

- Operationele activiteiten. Operationele afdelingen verzorgen de primaire bedrijfsprocessen van de organisatie (Organiseren van passende beheer- en beveiligingsmaatregelen). Denk aan verkoop, inkoop en productie of het leveren van zorg aan patiënten en vastleggen van de verrichtingen die vervolgens worden gefactureerd. Een bijzonder activiteit is het faciliteren van de technische infrastructuur (inrichting IT en processen). Een voorbeeld van dit soort infrastructuren is een netwerk waarmee computers en printers onderling verbonden zijn.

De aangebrachte structuur kan worden uitgewerkt in bedrijfsprocessen, deelprocessen en activiteiten. Binnen de structuur vinden wij de invalshoeken:

- Doel;
- Functies;
- Gedrag;
- Structuur.

Uit te werken voor systemen en verzamelingen van gegevens voor de organisatie zelf en de verwerkers en sub-verwerkers die namens de verwerkingsverantwoordelijke persoonsgegevens verwerken:

- Business architecturen;
- Financiële- en personeelsadministratie met daarin de (persoons)gegevens;
- Inkoopsysteem met daarin de (persoons)gegevens;
- Productiesysteem met daarin de (persoons)gegevens;
- Verkoopsysteem en CRM met daarin de (persoons)gegevens;
- Netwerken en beveiligingssystemen met daarin de (persoons)gegevens;
- En alle andere systemen die bedrijven en instellingen ter beschikking hebben de ondernemingsdoelstellingen te realiseren met daarin de (persoons)gegevens.

Op basis van het bovenstaande overzicht wordt duidelijk dat de persoonsgegevens “kleven” aan een reeks van interne en externe applicaties. De toegankelijkheid voor de betrokkene, het individu wordt hiermee ernstig gehinderd.

CONCLUSIE

Het verzamelen van het bewijs van effectieve werking van de beheers- en beveiligingsmaatregelen en hiervoor “*accountable*” te zijn voor het maatschappelijk verkeer wordt veelal ernstig bemoeilijkt door de bestaande organisatie van de gegevensverwerking en de informatievoorziening. De verwerkingsverantwoordelijke heeft in het netwerk van verwerkers en sub-verwerkers van persoonsgegevens te veel applicaties met “ingesloten” (persoons)gegevens. Een integraal overzicht en inzicht in de effectieve werking van de getroffen beheers- en beveiligingsmaatregelen is hiermee ook lastig of niet samen te stellen.

Om aan de verantwoordingsverplichting te voldoen en misschien wel belangrijker, te voorzien in de rechten van de betrokkene, moet er bij vele organisatie een omslag plaatsvinden. Een omslag die nodig is om in business te blijven en de continuïteit te behouden. In het proces van “*empowerment*” van de betrokkene is het erg belangrijk dat de (commerciële) relatie met de betrokkene, de klant, burger of patiënt in stand wordt gehouden en wordt versterkt. Digitale transformatie en Avg gaan volgens ons hand in hand om uw organisatie naar een klanttevredenheid te helpen die voorwaardelijk is voor het bestaansrecht van uw organisatie. Ook voor non-profit organisaties en in de zorg.

Het succes van een dergelijke business-transformatie hangt af van adequate voorbereiding. De centrale vraag is*: wat is de volwassenheid van mijn organisatie en welke stappen kan ik zetten*.

Duthler Associates
law, ICT & organisation

Afspraak maken en contact

Wilt u meer weten? Neem dan contact met ons op via de onderstaande gegevens.

Hoofdkantoor:

Frankenslag 137
2582 HH Den Haag

+31 (0) 70 392 22 09
info@duthler.nl
https://www.duthler.nl

Vestigingen

Den Haag
Eindhoven
Zwolle