



DIGITALE TRANSFORMATIE EN HET RECHT

Dit stuk is geschreven door: Ernst Jan Louwers en Natascha van Duuren

Voortschrijdende digitalisering, globalisering en een haast onbegrensde connected wereld stellen bestaande maatschappelijke verhoudingen op de proef. Daarbij komen dan nog de impact van de Covid-19 pandemie en wereldwijde handelsconflicten. Het belang van data en van toegang tot die data is meer dan ooit tevoren kraakhelder. Voor de ene organisatie raken de data direct de kern van de organisatie, voor de andere zal het wellicht de core business minder direct raken. Maar de beschikbaarheid van data geeft stellig een concurrentievoordeel (competitive advantage). Het woord 'data' omvat veel uiteenlopende soorten gegevens, variërend van persoonsgegevens, statistische analyses, financiële gegevens tot product sheets en gebruiksinformatie.

www.futurexl.nl/future-views

Hoe komt het nu dat sommige bedrijven er wél in slagen een succesvolle digitale transformatie door te maken en andere niet? Een belangrijke sleutel tot succes is een multidisciplinaire, holistische, aanpak en een goede governance en compliance zonder angst voor verandering. Digitale transformatieprojecten dienen vanaf het begin integraal te worden aanpakt. Cross silo denken is het sleutelwoord. Dat geldt ook voor de juridische aspecten. Het hele speelveld van digitale transformatie moet immers worden overzien, inclusief wet- en regelgeving. Bestaande juridische kaders zullen moeten worden toegepast om een verantwoorde kanteling van IT-technische naar data-centrische benadering in goede banen te leiden.

Juridische dilemma's bij digitale transformatieprojecten

Vanuit juridisch perspectief roepen digitale transformatieprojecten boeiende dilemma's op. Niet alleen ten aanzien van toenemend indringen in de persoonlijke levenssfeer en, wellicht onvermijdelijk, enige afkalving van privacy.

Ook andere dilemma's doen zich voor. Wie mag wat doen met data? Van wie zijn gegenereerde data eigenlijk? Kan iemand wel echt eigenaar zijn van afzonderlijke data?

Neem bijvoorbeeld een melkmachine: de fabrikant zal graag de data uit de machine willen gebruiken om zijn machines te verbeteren, maar de boer zal vinden dat de data van hem zijn. Hoe komt men tot een data sharing-model waarvan iedereen profiteert?

Verder zullen dit soort trajecten ook leiden tot interne en externe aanpassingen in bestaande rollen en contractuele verhoudingen.

Juridische aandachtspunten bij digitale transformatieprojecten: een stappenplan

Hieronder wordt ingegaan op de verschillende juridische issues in het kader van digitale transformatie. Dit is gedaan in de vorm van een globaal stappenplan, dat in beginsel toepasbaar is op alle digitale transformaties.

1. Maak een inventarisatie van het toepasselijk juridisch kader

Onvoldoende oog voor (de complexiteit van) toepasselijke wet- en regelgeving is een bekende pitfall bij digitale transformatieprojecten. Dat dit een bekende pitfall is, is goed te verklaren. De wet- en regelgeving heeft immers geen gelijke tred gehouden met de vlucht van technologische ontwikkelingen. Dit betekent dat verouderde wetgeving moet worden toegepast op nieuwe technologische ontwikkelingen. Ten tweede blijken diverse wetten en normen elkaar te overlappen. Interpretatie van deze lappendeken van wet- en regelgeving blijkt in de praktijk veel vragen op te roepen.

De wet- en regelgeving die bijvoorbeeld specifiek van toepassing is op 'data' (in de vorm van persoonsgegevens, bedrijfsgeheimen, databanken, et cetera) is complex en bovendien volop in ontwikkeling. Het juridische kader wordt bovendien gevormd door sector-specifieke regels en richtlijnen, bijvoorbeeld van de Autoriteit Financiële Markten (AFM) en De Nederlandse Bank (DNB). Voor het kiezen van de juiste strategie, het borgen van compliance en het treffen van de juiste beheersmaatregelen, is een grondig inzicht in deze regels en risico's noodzakelijk. Een te laat inzicht in het juridisch kader kan een organisatie duur komen te staan. Er zijn voorbeelden van bedrijven die kostbare applicaties hebben gebouwd of hebben laten bouwen, die vlak voor live-gang niet bleken te voldoen aan wettelijke eisen en die daarom van scratch af aan opnieuw moesten worden gebouwd. Het behoeft geen betoog dat dit een vorm van kapitaalvernietiging is die gemakkelijk voorkomen had kunnen worden door de juridische eisen vooraf te inventariseren en mee te nemen in de keuzes in het transformatieproject en het functioneel en technisch ontwerp. De wet eist in bepaalde gevallen zelfs compliance by design, vooral in gereguleerde markten als de financiële sector en gezondheidszorg. Denk bijvoorbeeld aan privacy by design op grond van de AVG.

2. Breng de bestaande legacy-systemen grondig in kaart

Werkelijke digitale transformatie zal leiden tot een grondige reshuffle van bestaande rollen en contracten, zowel intern met eigen personeel als extern met bestaande IT-leveranciers en outsourcingpartners. Het penny-wise pound-foolish vasthouden aan bestaande legacy-systemen kan in de weg staan aan het welslagen van digitale transformatieprojecten. Omdat de data-centrische benadering uitgaat van een fundamenteel ander startpunt, zullen de bestaande legacy-systemen veelal overboord moeten worden gegooid. En dat heeft tot gevolg dat het contractueel kader van de huidige architectuur volledig en nauwkeurig in kaart moet worden gebracht.

Cruciale vragen moeten worden gesteld om een helder en compleet beeld te krijgen van het bestaande IT-landschap en de juridische verhoudingen die daaraan hangen. Van welke applicaties wordt gebruikgemaakt? Is sprake van maatwerk, open source of standaardsoftware? Welke (licentie)voorwaarden zijn daarop van toepassing? Is sprake van outsourcing of cloud sourcing? Zijn er eigen of dedicated servers en staan deze intern of extern in datacenters?

Wat zijn de gevolgen van eventuele beëindiging van de licentie-, hosting- of onderhoudscontracten die hierop van toepassing zijn? Welke opzegtermijnen gelden? Van groot belang is of met de bestaande leveranciers afspraken zijn gemaakt over migratie en export van gegevens. De data zullen immers vanuit de applicatie- gedreven omgeving naar de nieuwe data-gedreven architectuur moeten worden gemigreerd. Dit vereist een goede en tijdige inventarisatie van de afspraken die hierover zijn gemaakt. Helaas wijst de praktijk uit dat een migratie naar een nieuw systeem en de bijbehorende datamigratie niet altijd over rozen gaat. De oude leveranciers weigeren vaak werkzaamheden uit te voeren zonder aanvullende vergoeding of voordat een vrijwaringsverklaring wordt getekend op basis waarvan zij volledig worden gevrijwaard voor alle schade die tijdens de migratie mocht ontstaan (waaronder verlies of beschadiging van data). Minder regelmatig komt het voor dat er technische belemmeringen blijken te zijn om een migratie succesvol uit te voeren.

Alle reden dus om de bestaande legacy-systemen en de daarmee samenhangende contracten tijdig en grondig in kaart te brengen.

3. Data due diligence

Bij de selectie van nieuwe applicatie(s) is het essentieel om te inventariseren welke data van strategisch belang zijn en welke wettelijke regels eventueel van toepassing zijn op het bezit en de verwerking van deze data. Dit houdt niet alleen verband met de eisen die aan de beveiliging van deze data moeten worden gesteld, maar ook met het feit dat te allen tijde moet worden gewaarborgd dat maximale controle kan worden gehouden op de beschikbaarheid en toegankelijkheid van strategische data.

Er dient in feite een data due diligence te worden uitgevoerd. Wat zijn mijn essentiële bedrijfskritische data? Waar zitten mijn essentiële data en hoe krijg ik die uit mijn oude systeem? Hoe zijn de data verkregen? Zijn zij rechtmatig verkregen? En wie mag zichzelf met recht de eigenaar noemen van bepaalde data? Is er wel een eigenaar aan te wijzen en op welke grond dan? Op grond van het databankenrecht of wellicht het octrooi- of auteursrecht? Welke rol speelt de Wet bescherming bedrijfsgeheimen? Welke rol speelt de AVG?

Het is dus zaak alle aanwezige data te 'minen' en in beeld te krijgen, zodat die data gemanaged (en adequaat beschermd) kunnen worden.

4. Denk aan eventuele personele consequenties

Een ingrijpend project als een ommezwaai naar een data-centrische organisatie kan gevolgen hebben voor de bezetting van bepaalde afdelingen, zoals de IT-afdeling. Zeker ook als sprake is van overgang naar cloudoplossingen. Indien dat het geval is, kunnen arbeidsrechtelijke aspecten aan bod komen die tijdig aandacht behoeven.

Mogelijk is zelfs de inmenging van de ondernemingsraad vereist. Indien dit aan de orde is, dient de ondernemingsraad tijdig te worden betrokken. Een ander arbeidsrechtelijk aspect kan zijn de vraag of sprake is van overgang van onderneming. Indien het uitbesteden van IT-werkzaamheden onderdeel van de digitale transformatie is, dan kan dit betekenen dat sprake is van overgang van onderneming en werknemers van de outsourcer automatisch in dienst zullen treden bij de insourcer. De werknemers volgen als het ware het werk. Ook deze eventuele consequenties zullen vooraf moeten worden geïnventariseerd.

5. Breng de (wettelijke) eisen in kaart die worden gesteld aan het verzamelen van data, zoals informatiebeveiliging en privacy

De regels op het gebied van informatiebeveiliging en privacy zijn streng en worden steeds strenger. Het is van groot belang te voldoen aan deze regels. Niet alleen met het oog op boetes die door de toezichthoudende autoriteiten kunnen worden opgelegd, maar ook met het oog op het verliezen van het vertrouwen van klanten. Onrechtmatige verwerking van klantgegevens en/of een datalek kunnen immers desastreus zijn voor het imago van een organisatie. In een nieuwe (data-centrische) situatie is het niet alleen belang grip op de data te houden, maar ook te waarborgen dat de informatiebeveiliging op orde is. Onder informatiebeveiliging wordt verstaan het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit, alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.

Voor sommige sectoren zal voldaan moeten worden aan sector-specifieke informatiebeveiligingsrichtlijnen en -voorschriften. Denk bijvoorbeeld aan de financiële sector, telecom en gezondheidszorg. Die eisen moeten vooraf in kaart worden gebracht, zodat zij tijdig kunnen worden meegenomen bij het ontwerp en inrichting van de nieuwe data-centrische situatie.

6. Data als voorwerp van intellectueel eigendom

Data en dataverzamelingen kunnen een intellectueel asset en zelfs balanswaarde vertegenwoordigen. Daarvoor moeten de data natuurlijk wel helder in beeld zijn: het moet duidelijk zijn wat het betreft. Data kunnen allereerst onder bepaalde voorwaarden beschermd zijn als databank. Daarvoor is in essentie vereist dat de data zijn ondergebracht in een systematisch geordende en doorzoekbare verzameling van gegevens. Bovendien moet in die databank substantieel zijn geïnvesteerd om te kwalificeren als databank in de zin van de Databankenwet.

Verder kunnen data octrooieerbare technische informatie bevatten of bijvoorbeeld informatie over plantveredeling die eventueel recht geeft op kwekersrecht op een gevonden ras. Gegevens over vormgeving kunnen leiden tot een modelrecht en/of auteursrecht. En namen en logo's kunnen merkrechten vertegenwoordigen.

Ook trade secrets zijn te beschouwen als data die nogal eens de kroonjuwelen van de organisatie belichamen. Dat kan bijvoorbeeld variëren van gegevens over commerciële strategieën en modellen tot meer technische productiemethoden, werktekeningen en cruciale informatie over logistieke processen. Trade secrets zou men kunnen zien als pseudo-intellectueel eigendom. Bedrijfsgeheimen zijn in zekere mate en onder voorwaarden beschermd. Daarvoor is onder andere vereist dat deze geheim worden gehouden met passende organisatorische, juridische en technische maatregelen. Bij digitale transformatie dient men ook daarmee rekening te houden.

7. Zorg voor heldere contracten

Een succesvol project vereist goede contracten met een heldere verdeling van de taken, verantwoordelijkheden en risico's van de betrokken partijen. Daarbij horen duidelijke afspraken over budget, programma van eisen, KPI's en service levels.

Vandaag de dag is een digitale transformatie zonder cloud- en platformoplossingen nauwelijks meer denkbaar. Cloud- en platformoplossingen zijn steeds vaker verbonden met AI, Internet of Things (IoT), Big data en blockchain. Dat maakt de verdeling van taken, verantwoordelijkheden en risico's operationeel én juridisch een stuk complexer (maar ook boeiender). Zeker ook omdat de technische eisen ook steeds sneller wijzigen. Dat kan een van de redenen zijn om een digitale transitie als Agile/Scrum-project in te steken.

Ook bij een Agile/Scrum-projectaanpak is een goed contract essentieel. Ook dan moet immers worden gewaarborgd dat te allen tijde grip kan worden gehouden op de dienstverlening van een leverancier.

8. Regel contractmanagement in

Gedurende de contractperiode dient consequent contractmanagement te worden uitgevoerd. Worden afspraken nagekomen? Welke contractuele escalatie- mogelijkheden dienen te worden gevolgd? Worden changes op een juiste wijze doorgevoerd? Of, in geval van een Agile/Scrum-aanpak, worden de sprints correct afgesloten voordat wordt doorgedaan naar de volgende sprint?

De rol van contractmanagement wordt in de praktijk helaas vaak onderschat en verwaarloosd. Ook in een data- centrische omgeving zal gebruik gemaakt worden van applicaties van leveranciers. Zij hebben feitelijk vaak (contractuele) (stuur-) middelen in handen die ook de (kritische) data kunnen raken. Daardoor kan de klant in een niet benijdenswaardige vendor-lockin verzeild raken. Met goede maatregelen zoals redundancy, periodieke datadump en goede exit-afspraken kan men het risico verminderen als klant gegijzeld te worden door de IT-leverancier.

Checklist voor bestuurders

Op basis van bovenstaande juridische aandachtspunten is hieronder een basale checklist opgenomen van (juridische) punten die bij een stevig digitaal transformatieproject doorgaans aan de orde zullen komen:

1. Wat is het einddoel van de digitale transformatie?
2. Wat zijn de belangrijkste eisen die worden gesteld aan de nieuwe situatie?
3. Wat is de roadmap naar de nieuwe situatie?
4. Welke relevante legacy-systemen en welke applicaties zijn er nu en welke worden overbodig?
5. Welke overeenkomsten bestaan er met toeleveranciers ten aanzien van de relevante bestaande legacy-systemen en applicaties die overbodig worden?
6. In hoeverre grijpt de transformatie in op de eigen personele bezetting?
7. Wat voor data worden geraakt door het project?
8. Hoe werden of worden de data verkregen?
9. Is en wordt aantoonbaar substantieel geïnvesteerd in de data en de verzameling en/of onderhoud of verrijking daarvan?

10. Hoe worden de relevante data straks ontsloten?
11. Worden de data uitsluitend intern gebruikt of (ook) extern gedeeld?
12. Wie is te beschouwen als 'eigenaar' en beheerder van de data?
13. Betreffen de data (ook) persoonsgegevens? Zijn het data die vallen onder specifieke regelgeving in een gereguleerde sector?
14. Wie heeft nu toegang en krijgt straks toegang tot de data?

Ter afsluiting

- Bepaal voorafgaand het doel van en de eisen aan de digitale transformatie, inclusief juridische eisen.
- Maak een legal roadmap en borg legal compliance.
- Maak iemand verantwoordelijk voor de legal compliance en governance



Contact

Kom direct in contact met onze managing director Ken van Ierlant en bespreek wat FutureXL voor uw bedrijf kan betekenen.

Telefoon

(06) 201 693 60

E-mail

ken@futurexl.nl

Adres

Boeingavenue 222,
1119 PN Schiphol Rijk
Nederland