Kwaliteit en informatiebeveiliging binnen Daywize

01-01-18 Edwin Bronts

Inhoud

1 Inleiding

Kwaliteit

Risicobeheersing is van essentieel belang voor de continuïteit van de bedrijfsvoering van Daywize. Ons vak draait namelijk in hoge mate om vertrouwen. Als HR service provider beheren wij immers het grootst denkbare kapitaal van elke organisatie: de gegevens van het personeel! U wilt dat u gegevens bij ons veilig verwerkt worden en wij u de producten en services bieden tegen het kwaliteitsniveau die we hebben afgesproken. Graag lichten wij u in dit beleidsdocument toe hoe het kwaliteitsmanagementsysteem van Daywize in elkaar steekt.

Informatiebeveiliging

Informatiebeveiliging vormt een onderdeel van het kwaliteitsmanagementsysteem van Daywize.
Zowel wijzelf als onze klanten zijn dagelijks afhankelijk van de beschikbaarheid van betrouwbare informatie waar gezien de aard van de data vertrouwelijk mee om moet worden gegaan. Onze organisatie en onze informatievoorziening worden blootgesteld aan bedreigingen, al dan niet opzettelijk van aard. Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren.

Beleid

Het proces van kwaliteit en informatiebeveiliging begint met het definiëren van een beleid op dit punt. Losstaande interne richtlijnen zijn op 18 september 2014 door de directie van Daywize vastgesteld in beleid dat is vastgelegd in dit document. Door de gewijzigde wet- en regelgeving heeft in januari 2016 en januari 2018 een aanpassing plaatsgevonden.

Certificering

Transparantie is een van onze kernwaarden. Wij laten dan ook graag door onafhankelijke derden toetsen of datgeen wat we beleidsmatig opschrijven ook dagelijks in de praktijk brengen. Daarom zijn we gestart met het implementeren van de ISO 9001 en 27001 standaarden die we door een onafhankelijk auditor laten certificeren. We hopen dit traject in 2018 positief af te ronden.

Ik wens u veel leesplezier.

Edwin Bronts
Directeur Daywize

2 Kwaliteitsmanagementsysteem Daywize

2.1 Criteria ISO 9001 als minimaal kader, waarden als leidraad

Om diensten van een hoge kwaliteit te kunnen leveren werkt Daywize met een kwaliteitsmanagement-systeem dat voldoet aan de criteria van NEN ISO 9001:2015. Het kwaliteitsmanagementsysteem bevordert de professionaliteit van onze organisatie en stelt zeker dat wij onze klanten consistent een kwalitatief hoogwaardig product of dienst verlenen zoals deze contractueel zijn afgesproken. Zo moet een organisatie conform de ISO 9001 norm:

- er voor zorgen dat werkzaamheden gepland uitgevoerd worden
- er voor zorgen dat de ontwikkeling en implementatie van software beheerst wordt uitgevoerd
- de manier waarop software en diensten tot stand komen bewaken
- acties ondernemen om softwarefouten te beheersen en problemen op te lossen
- acties ondernemen om problemen te voorkomen
- registraties (administraties) er op nahouden van bepaalde in de norm beschreven activiteiten (zoals klachten en contractbeoordeling)
- invulling geven aan een aantal in de norm vastgelegde processen/activiteiten
- zorgen voor een kwaliteitsmanagementsysteem waarin een aantal beschreven relevante documenten zijn vastgelegd
- risico's identificeren en beperken

Daarbij voldoen wij uiteraard ook aan wettelijke en overige van toepassing zijnde eisen.

Maar wij willen verder gaan. Door onze klanten en partners in alle processen centraal te stellen willen we hun verwachtingen overtreffen! Door ons te concentreren op het "in een keer goed doen" en te leren van onze fouten en die van onze klanten en partners. Door eerlijk en transparant te zijn over wat we wel en niet op een bepaald moment ondersteunen of wat je wel of niet als klant of partner moet willen. Door flexibel te zijn als dat kan, en een klant of partner niet te zien als een optelsom van licenties. Door innovaties aan te brengen in onze primaire processen waarvan onze klanten en partners nog niet wisten dat ze er blij van zouden worden.

daywize FIT

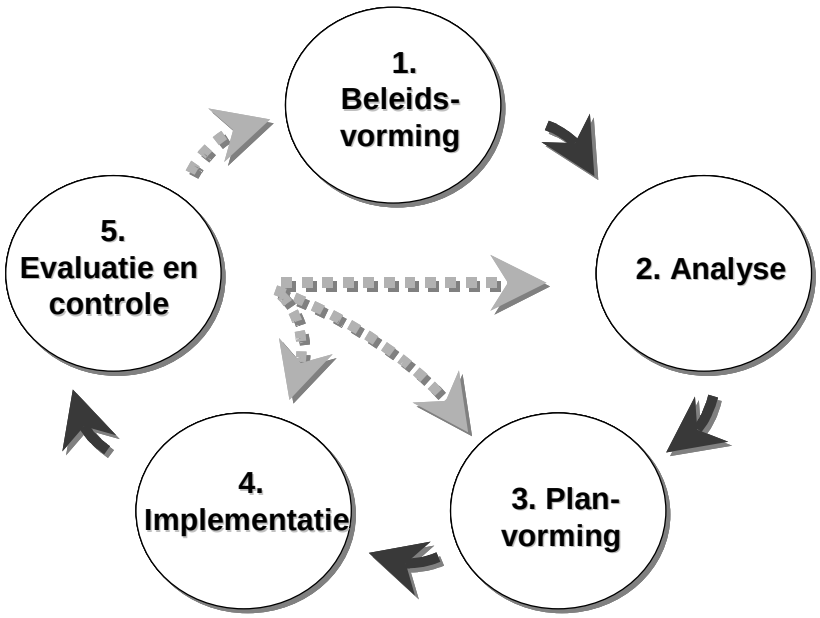
FLEXIBEL I INNOVATIEF I TRANSPARANT

Deze primaire processen bestaan bij Daywize uit het ontwikkelen, verkopen, implementeren en supporten van state-of-the-art software en services. Waarbij onze eigen drive naar perfectie, projectevaluaties, klachten, bevindingen uit audits en klanttevredenheidsonderzoeken de zuurstof vormen voor continue verbetering.

2.2 Proces van continue verbetering

Het kwaliteitsmanagementsysteem van Daywize is conform de ISO standaarden 9001 en 27001 gebaseerd op een proces dat zich richt op continue verbetering.

Dit continue proces bevat de volgende vijf stappen:



1. Beleidsvorming

Het proces start met het opstellen van beleid. In dit beleid worden de doelstellingen en uitgangspunten voor kwaliteit en informatiebeveiliging van Daywize vastgelegd. Hiermee vormt het beleid de leidraad voor de overige stappen van het proces.

2. Analyse

De tweede stap van het proces voor kwaliteit en informatiebeveiliging bestaat uit analyse van de bestaande situatie. Het analyseren van de bestaande situatie heeft tot doel:

- Inzicht te krijgen in de kwaliteit van de primaire processen en bestaande beveiligingsmaatregelen;
- Inzicht te krijgen in de risico's binnen de primaire processen en/of risico's die de realisatie van het gewenste beveiligingsniveau in gevaar kunnen brengen;
- Het gewenste kwaliteitsniveau van processen en informatiebeveiliging vast te stellen in de vorm van een classificatie van bedrijfsprocessen, informatiesystemen en gegevensverzamelingen.

Over de uitkomsten van de analyse van de bestaande situatie van de kwaliteit binnen de primaire processen en informatiebeveiliging wordt periodiek gerapporteerd aan de CEO.

3. Planvorming

Op basis van de uitkomsten van de analyse van de bestaande situatie wordt een verbeterplan opgesteld. In dit plan worden de verbeteractiviteiten voor de realisatie op projectmatige wijze vastgelegd.

4. Implementatie

Aan de hand van het verbeterplan wordt de implementatie van de aanvullende maatregelen ter hand genomen. Dit kan bijvoorbeeld bestaan uit het opstellen en/of aanpassen van richtlijnen en werkprocessen en/of informatiebeveiliging, het invoeren van beveiligingshulpmiddelen en het voorlichten en opleiden van management en medewerkers.

5. Evaluatie en controle

Een van de ISO-eisen is dat de organisatie zorgt voor de opzet van een doeltreffend en doelmatig auditproces om sterke en zwakke punten van het kwaliteitssysteem binnen de organisatie te beoordelen. Het auditproces is een managementinstrument voor onafhankelijke beoordeling en om bewijs te verkrijgen dat aan bestaande eisen binnen de normering is voldaan. De audits evalueren de doeltreffendheid en doelmatigheid van de organisatie. Een goedlopend intern auditproces borgt een goede voorbereiding voor externe audits. De afspraken over de kwaliteitsbewaking zijn vastgelegd in het auditbeleid.

2.3 Digitaal kwaliteitshandboek

In hoofdlijnen vraagt de ISO 9001 norm dat Daywize vastlegt hoe processen worden beheerst en dat we de benodigde middelen beschikbaar stellen om producten volgens klanteisen te leveren. De norm vraagt om bewaking van processen en producten en analyse van de resultaten zodat continue verbeteringen mogelijk zijn.

Gelukkig is deze materie ons niet vreemd! In onze dagelijkse dienstverlening vertalen wij continu personeelsbeleid via concrete doelstellingen naar procesbeschrijvingen, taken en verantwoordelijkheden, werkafspraken en rapportages om op het geformuleerde personeelsbeleid te kunnen sturen. En zorgen voor bijpassende digitale tools om dit geheel te ondersteunen. In het kader van kwaliteit hebben we dit ook voor onze eigen primaire processen gedaan. Dit betekent dat alle medewerkers binnen Daywize digitaal toegang hebben tot onze beleidsdocumenten, kwaliteitsdoelen, procesbeschrijvingen / procedures / werkinstructies, taken / verantwoordelijkheden, gesignaleerde risico's en verbeteracties, audits, etc.

3 Informatiebeveiliging

3.1 Definities, doelstellingen en uitgangspunten

Informatiebeveiliging wordt door ons als volgt gedefinieerd:

> **Het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen.**

Binnen Daywize omvat informatiebeveiliging een *samenhangend stelsel* van maatregelen. Dit betekent dat de verschillende maatregelen die tezamen de informatiebeveiliging vormen niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan. Het stelsel van beveiligingsmaatregelen heeft tot doel een *blijvend niveau van beveiliging* te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn blijft gehandhaafd. Informatiebeveiliging is gericht op het realiseren van een *optimaal niveau van beveiliging.* Dit optimum wordt bereikt door een zorgvuldige afweging van kosten en baten, wet- en regelgeving en gebruikersgemak.

Doelstelling informatiebeveiliging

Het opstellen van het informatiebeveiligingsbeleid heeft tot doel de doelstellingen en uitgangspunten met betrekking tot informatiebeveiliging binnen Daywize vast te stellen en vast te leggen. Hiermee vormt het beleid de leidraad voor alle betrokkenen bij informatiebeveiliging binnen Daywize. Het informatie-beveiligingsbeleid maakt onderdeel uit van het kwaliteitsmanagementsysteem dat binnen Daywize gehanteerd wordt. Zoals in de voorgaande definitie is verwoord, richt informatiebeveiliging zich op de volgende drie aspecten van de informatievoorziening:

- *Beschikbaarheid*, de informatie moet op de gewenste momenten beschikbaar zijn;
- *Integriteit*, de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- *Vertrouwelijkheid*, de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is.

Werkingsgebied

Het informatiebeveiligingsbeleid is van toepassing op de gehele organisatie en dienstverlening vanuit Daywize. Het informatiebeveiligingsbeleid is ook van toepassing op de gegevensuitwisseling van Daywize met andere organisaties. Het beleid richt zich op onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie.

Uitgangspunten

Naast het doel en de reikwijdte van informatiebeveiliging heeft Daywize de volgende uitgangspunten voor de interne organisatie gedefinieerd:

- Informatie wordt beschikbaar gesteld op basis van het 'need to know' principe. Dit houdt in dat een medewerker niet meer informatie tot zijn of haar beschikking mag krijgen dan voor het uitvoeren van zijn of haar werkzaamheden noodzakelijk is;
- Management en medewerkers dienen zich bewust te zijn van de noodzaak van informatiebeveiliging en zorgen dat het beleid en de genomen maatregelen nageleefd worden;

- Informatiebeveiliging is zoveel mogelijk een onderdeel van de normale bedrijfsprocessen en zo weinig mogelijk belastend voor de normale werkzaamheden van de medewerkers;
- Informatiebeveiliging is een geïntegreerd onderdeel van de besturing van Daywize. Daywize heeft de ambitie om continue "in control te zijn" ten aanzien van informatiebeveiliging;
- Informatiebeveiliging gaat uit van het feit dat voorkomen beter is dan genezen. Dit betekent dat zoveel mogelijk preventieve maatregelen worden getroffen;
- Voldoen aan alle regelingen van haar klanten. Getroffen beveiligingsmaatregelen hebben als doel om te voldoen aan - voor Daywize relevante - bepalingen in overeenkomsten met klanten;
- In alle gevallen waarin het beleid voor informatiebeveiliging niet voorziet beslist de directie van Daywize wat het beleid is.

3.2 Rollen en verantwoordelijkheden informatiebeveiliging

Het is van groot belang dat de verantwoordelijkheden, taken en bevoegdheden met betrekking tot informatiebeveiliging op een eenduidige wijze zijn toegewezen. Deze toewijzing heeft tot doel te voorkomen dat zaken dubbel worden uitgevoerd of dat de uitvoering van beveiligingstaken achterwege blijft. Bovendien levert de toewijzing van taken en verantwoordelijkheden binnen Daywize de mogelijkheid om decharge te verlenen voor de uitgevoerde werkzaamheden.

Bij het gebruik van een applicatie uit de Daywize Cloud zijn verschillende partijen betrokken:
1. De klant die de HR software afneemt.
2. Een leverancier die de HR software levert (Daywize). Deze dienst wordt ook wel ‘software as a service’ genoemd (SAAS).
3. Een leverancier die een applicatieplatform levert (Mendix). Deze dienst wordt ook wel ‘application platform as a service’ genoemd (aPAAS). Lees meer hierover in bijlage C.
4. Een leverancier die de hosting vanuit een beveiligd datacentrum verzorgt (bijvoorbeeld Amazon Web Services). Deze dienst wordt ook wel ‘infrastructure as a service’ genoemd (IAAS).

Personen kunnen verschillende rollen vervullen en deze rollen liggen zoals zojuist geschetst ook grotendeels buiten Daywize. De verschillende betrokkenen hebben onderling afspraken gemaakt over de uitvoering van de (beveiligings-)taken die zijn vastgelegd in dienstverleningsovereenkomsten (SLA’s) en (sub-)verwerkersovereenkomsten. Zo heeft de klant een SLA en verwerkersovereenkomst met Daywize, Daywize een SLA en sub-verwerkersovereenkomst met Mendix en Mendix op haar beurt weer met de hostingpartijen waarmee zij samenwerken. De verantwoordelijkheden zijn als volgt belegd:

Stakeholder	Rol	Verantwoordelijkheden
Klant	Verantwoordelijke	• Beslissingsrecht voor het informatiesysteem, c.q. de gegevensverzameling, opstellen verwerkingsregister • Bepalen van de beveiligingseisen
Klant	Functioneel beheerder	• Ondersteunen van de verantwoordelijke bij het bepalen van de beveiligingseisen
Klant	Applicatiebeheerder / Databasebeheerder	• Operationeel in stand houden van het informatiesysteem, c.q. de gegevensverzameling • Toezien op een juiste werking van het informatiesysteem, c.q. de gegevensverzameling
Klant	Gebruiker / Betrokkene	• Toepassen van het informatiesysteem, c.q. de gegevensverzameling • Naleven van beveiligingsrichtlijnen en -procedures

Stakeholder	Rol	Verantwoordelijkheden
Daywize	CEO	• Vaststellen en evalueren van beveiligingsbeleid • Toezien op compliance security in contracten partners
Daywize	Teamleader Development	• Opstellen van beveiligingsbeleid • Goedkeuren van beveiligingsinitiatieven • Contact opnemen met officiële instanties ingeval van beveiligingsincidenten
Daywize	HR verantwoordelijke	• Inregelen HR-processen die het beveiligingsbeleid raken
Daywize	ICT verantwoordelijke	• Goedkeuren van middelen voor informatievoorziening • Beschermen van bedrijfsmiddelen
Daywize	Security Officer	• Uitvoeren interne audits • Toezien op en bespreken van beveiligingsincidenten
Daywize	Projectmanager / Testcoördinator	• Uitvoeren van voor informatiebeveiliging relevante test- en implementatieprocessen
Daywize	Ontwikkelaar	• Ontwikkelen van applicaties in Daywize Cloud, c.q. de gegevensverzameling, conform de beveiligingseisen die zijn gesteld • Actief meedenken over de realisatie en de beveiliging van applicaties in Daywize Cloud, c.q. de gegevensverzameling • Signaleren van nieuwe bedreigingen • Toepassen 'Privacy by Design' uitgangspunten
Mendix	CEO	• Vaststellen en evalueren van beveiligingsbeleid • Toezien op compliance security in contracten partners
Mendix	CTO	• Opstellen van beveiligingsbeleid • Goedkeuren van beveiligingsinitiatieven
Mendix	HR verantwoordelijke	• Inregelen personeelsprocessen die het beveiligingsbeleid raken
Mendix	ICT verantwoordelijke	• Goedkeuren van middelen voor informatievoorziening • Beschermen van bedrijfsmiddelen
Mendix	Security Officer	• Uitvoeren interne audits organiseren extern audits • Toezien op en bespreken van beveiligingsincidenten • Contact opnemen met officiële instanties ingeval van beveiligingsincidenten
Mendix	Hoofd R&D / Testcoördinator	• Uitvoeren van voor informatiebeveiliging relevante test- en implementatieprocessen
Mendix	Ontwikkelaar	• Ontwikkelen Mendix framework, c.q. de gegevens-verzameling, conform de beveiligingseisen die zijn gesteld • Signaleren van nieuwe bedreigingen
Mendix / Hostingpartij	Technisch beheerder	• Exploitatie en ontsluiting van de technische infrastructuur • Toezien op een juiste technische werking van de technische infrastructuur

In de volgende sub paragrafen beschrijven wij de beveiligingsaspecten per betrokken partijen (exclusief de klant) aan de hand van de indeling People / Process / Technology.

4.1.1 Daywize Cloud (SAAS)

Het kwaliteitssysteem van Daywize is ontwikkeld op basis van de ISO 9001 standaard. De project-methodiek is gebaseerd op een plan van aanpak pakketimplementatie dat ontwikkeld is door EY.

People – Personeelsbeleid Daywize

Aan de volgende vereisten en plichten dienen het personeel en ingehuurden van Daywize zich te voldoen in relatie tot het informatiebeleid:

- **Opleiding & ervaring**
  Consultants bij Daywize moeten voldoen aan één van de volgende (opleidings-)eisen:
  Een afgeronde HBO- of universitaire opleiding. Minimaal vijf jaar ervaring in middelgrote of grote organisaties en in het bezit van certificaten die aantonen dat de persoon voldoende theoretische basis heeft. Technische consultants / ontwikkelaars zijn Mendix gecertificeerd of zitten in het traject om deze certificering te behalen.

- **Verklaring omtrent het gedrag**
  Voordat personeel in aanmerking komt voor een functie binnen Daywize zal eerst een verklaring omtrent het gedrag moeten worden overhandigd.

- **Meldplicht**
  Het personeel van Daywize heeft een meldplicht voor het melden van beveiligingsincidenten. Deze meldingen worden vervolgens door de desbetreffende rolverantwoordelijke zo snel mogelijk opgepakt.

- **Geheimhouding**
  Al het personeel is gebonden aan een geheimhoudingsverklaring die is opgenomen in het arbeidscontract. Ingehuurden dienen voor aanvang van hun werkzaamheden eerst een aparte geheimhoudingsverklaring te tekenen.

Process – Live brengen klantomgeving Daywize Cloud

Het ontwikkelen van klantspecifieke applicaties gebeurt volgens de OTAP-strategie (Ontwikkel, Test, Acceptatie, Productie). Bij het live brengen van een klantomgeving in de Daywize Cloud heeft de klant de keuze om de testomgeving niet af te nemen. Per fase komen de relevante beveiligingsaspecten aan bod:

1. **Ontwikkelingsomgeving**
   Eerst wordt de applicatie lokaal ontwikkeld waarbij de ontwikkeldatabases lokaal worden opgeslagen. Deze databases zijn gelijkwaardig aan de productieomgeving en worden alleen op media met hardwarematige encryptie opgeslagen of in een crypto container.

2. **Testomgeving / Acceptatieomgeving**
   Wanneer de ontwikkelaar zelf zijn applicatie getest heeft wordt deze op een test- of acceptatie-omgeving geplaatst in de Daywize Cloud. Alleen geautoriseerde projectleden hebben toegang tot deze omgevingen. De Daywize Cloud is alleen over een https-verbinding bereikbaar en is qua veiligheid gelijk aan een productieomgeving. De reden hiervoor is dat bij acceptatietesten de applicatie op een database dient te draaien die gelijkwaardig is aan de productieomgeving. Pas nadat de klant de applicatie heeft goedgekeurd wordt deze naar de productieomgeving verplaatst. Het maken van back-ups van een omgeving wordt gelogd en kan alleen door bevoegd Daywize-personeel uitgevoerd worden.

3. Productie-omgeving

Back-ups worden automatisch elke nacht gemaakt. De volgende back-ups worden bewaard:

- Nachtelijke back-ups: maximaal 2 weken historie (tellend vanaf gisteren)
- Zondagse back-ups: maximaal 3 maanden historie (tellend vanaf gisteren)
- Maandelijkse back-ups (eerste zondag van elke maand): maximaal 1 jaar historie

Wanneer back-ups lokaal worden opgeslagen voor testdoeleinden, dan gebeurt dit altijd op media met hardwarematige encryptie of in crypto containers.

Enkel de projectmanager is bevoegd om personeel en/of ingehuurde externen toe te wijzen aan een projectteam. De technisch projectleider dient voordat iemand daadwerkelijk rechten krijgt dit altijd te valideren.

Technology – Beveiliging Daywize Cloud

- **Autorisaties**
  Applicatie in de Daywize Cloud werken op 'rol' gebaseerde autorisaties. Gebruikers krijgen een rol toegewezen, die weer is gekoppeld aan 'privileges'. Alleen gebruikers met een passend niveau van privileges kunnen bepaalde acties en/of taken uitvoeren. Privileges kunnen op verschillende niveaus worden bepaald: applicatieniveau, formulierniveau, rapportageniveau en tabelniveau. Per applicatie maken wij een onderscheid in read-, insert-, update- en delete rechten. Alleen gebruikers met voldoende rechten kunnen wijzigingen aanbrengen in de privileges (denk aan de applicatiebeheerder). De beveiliging middels autorisaties zorgt ervoor dat gebruikers alleen kunnen doen wat voor hen is "toegestaan" te doen in de applicatie. Alle andere handelingen die de gebruiker uitvoert, worden automatisch geblokkeerd door het systeem.

- **Auditing**
  Bij het onderhouden en op klantverzoek verder ontwikkelen van applicaties binnen de Daywize Cloud maakt Daywize gebruik van de auditing-oplossing. Deze oplossing zorgt ervoor dat aangebrachte wijzigingen in de applicatie, op object (tabel)niveau worden gelogged. Door het 'loggen' kunnen wijzigingen worden getraceerd, zowel op applicatie- als op gebruikersniveau. De Teamleider Development van Daywize is eindverantwoordelijk voor de doorontwikkeling van de modules / applicaties binnen Daywize Cloud en controleert zowel via de ontwikkelaars als de testcoördinator of alle gedefinieerde beveiligingstests op productniveau volledig zijn gedefinieerd en afgetest.

4.1.2 Mendix App Platform (aPaas)

Daywize Cloud is ontwikkeld op het Mendix App Platform. Mendix implementeert relevante marktstandaarden met betrekking tot beveiliging en beschikt over een ISO 27001 en een ISAE 3402 type 2 certificering.

Mendix applicaties worden door heel diverse klanten ingezet om zeer diverse bedrijfsprocessen te automatiseren. Wat al deze klanten gemeenschappelijk hebben, is de eis dat de toepassingen die ze installeren veilig en toegankelijk zijn. Ook als de applicatie in de cloud gehost wordt, vindt Mendix dat klanten er vanuit moeten kunnen gaan dat hun gegevens minstens net zo veilig zijn als binnen hun eigen netwerk. Mendix wordt ingezet bij klanten die met zeer vertrouwelijke informatie te maken hebben. Organisaties zoals ABN AMRO, Dun & Bradstreet, Achmea, TNT en PKN vertrouwen op Mendix voor online transacties, bewaren of aanpassen van medische of verzekeringsgegevens, internationale overboekingen en andere kritische processen en informatiestromen.

People – Personeelsbeleid Mendix

Aan de volgende vereisten en plichten dient het personeel en ingehuurden van Mendix zich aan te voldoen in relatie tot het informatiebeleid:

- **Opleiding & ervaring**
  Systeembeheerders bij Mendix moeten voldoen aan één van de volgende (opleidings)eisen:
  Een HBO of universitaire opleiding informatica met een major in systeembeheer. Minimaal vijf jaar systeembeheerervaring in middelgrote of grote organisaties en in het bezit van certificaten die aantonen dat de persoon voldoende theoretische basis heeft.

- **Verklaring omtrent het gedrag**
  Voordat personeel in aanmerking komt voor de functie systeembeheerder zal eerst een verklaring omtrent het gedrag moeten worden overhandigd.

- **Meldplicht**
  Het personeel van Mendix heeft een meldplicht voor het melden van beveiligingsincidenten. Deze meldingen worden vervolgens door de desbetreffende verantwoordelijke manager zo snel mogelijk opgepakt.

- **Geheimhouding**
  Al het personeel is gebonden aan een geheimhoudingsverklaring die is opgenomen in het arbeidscontract. Ingehuurden dienen voor aanvang van hun werkzaamheden eerst een aparte geheimhoudingsverklaring te tekenen.

Process – Releasemanagement Mendix Platform

Voordat er een nieuwe versie van het Mendix framework wordt uitgebracht wordt de technologie eerst volgens het Mendix release testplan getest, waarbij gecontroleerd wordt of alle security features binnen de test naar behoren werken. Deze tests worden uitgevoerd door het testteam van de Reseach & Development (R&D) afdeling van Mendix.

Technology – Beveiliging Mendix Platform

We beschrijven hier op hoofdlijnen welke beveiligingsmaatregelen in het Mendix platform zijn doorgevoerd. Voor een uitgebreid overzicht van de beveiliging(smogelijkheden) verwijzen we naar de Mendix Security whitepaper in bijlage D. Een groot deel van de veiligheid van de modules / applicaties in de Daywize Cloud wordt aangedreven door het Mendix Platform waarop deze zijn ontwikkeld:

- **Authenticatie**
  Mendix applicaties volgen een ‘entry-point’ authenticatie. De gebruiker wordt bij het inloggen geverifieerd met een gebruikersnaam en wachtwoord. Alleen bij succesvolle authenticatie zal de gebruiker toegang krijgen tot de applicatie. Standaard worden beveiligingstokens toegekend tijdens succesvol inloggen. De tokens worden tijdens elk volgend verzoek aan de server gecontroleerd. Een onbevoegde gebruiker kan dus nooit toegang hebben tot de ‘binnenkant’ van het systeem.

- **Wachtwoordbeveiliging**
  Gebruikers loggen in met gebruikersnaam en wachtwoord. Alleen de beheerder aan de klantzijde kan een wachtwoord wijzigen van een gebruiker.

- **SSL-ondersteuning / SSH / FTP**
  Mendix applicaties bieden volledige ondersteuning voor SSL (HTTPS). SSL zorgt er voor dat alle communicatie tussen de browser van de klant en de server wordt versleuteld: veilig en tamper proof.

Iedere Daywize Cloud omgeving heeft dan ook een beveiligde omgeving voorzien van SSL certificaat. Onderhoud van de server is alleen mogelijk via het Secure Shell Protocol (SSH) waarbij een verbinding wordt gemaakt middels een unieke digitale key. Upgrades kunnen alleen worden doorgevoerd via een beveiligde FTP-connectie die data transporteert over de SSH-verbinding.

De CTO van Mendix is eindverantwoordelijk voor de doorontwikkeling van het Mendix platform en controleert zowel via het hoofd van de R&D afdeling als de testcoördinator of alle gedefinieerde beveiligingstests op productniveau volledig zijn gedefinieerd. Verder bewaakt releasemanagement software het releaseproces, zodat er geen software uitgebracht kan worden die niet door alle gedefinieerde (beveiligings-)testen heen is gekomen.

4.1.3 Hosting (IAAS)

Daywize neemt hosting af via Mendix die de omgevingen optimaliseert in professionele datacentra uit de top van de hostingmarkt. Deze partijen beschikken over alle gebruikelijke certificeringen. De beveiligingsaspecten voor de infrastructuur zijn in verschillende niveaus van toegang te onderscheiden:

- **Fysieke toegang tot de serverruimte**
  Afhankelijk van het hostingscenario wordt er gebruikt gemaakt van een cloud omgeving of een dedicated colocation omgeving. Fysieke toegang tot de serverruimte voor de cloud omgeving is beperkt tot medewerkers van de leverancier. De toegang voor de dedicated colocation omgeving is beperkt tot medewerkers van het team binnen Mendix dat verantwoordelijk is voor het technisch beheer van de hostingomgeving.

- **Toegang tot apparatuur en besturingssysteem op beheer-niveau**
  Toegang op beheer-niveau tot apparatuur die geplaatst is in de hostingomgeving is voorbehouden aan de medewerkers van het technisch beheer. Dit team garandeert dat het beheer op afstand (zonder dat fysieke toegang nodig is) van alle apparatuur zo optimaal mogelijk is ingericht. Voor de beheertoegang op afstand wordt onder andere gebruik gemaakt van faciliteiten die de complete controle bieden over de omgeving waarbij de noodzaak tot fysiek bezoek geminimaliseerd wordt.

Daywize Cloud draait in professionele datacentra in Nederland en/of Europa. Desgewenst kunnen wij nadere informatie verschaffen over de betreffende leveranciers/locaties en hun beveiligingsbeleid.

4 Privacy en wet- en regelgeving

4.1 Privacy

Daywize voert een actief beleid op het punt van de bescherming en bewaking van de privacy van gebruikers van haar applicaties:

- **Gegevens worden zonder toestemming nooit doorgegeven aan derden**
  Uitgangspunt voor het privacybeleid is dat alle in de door Daywize ontwikkelde applicaties opgenomen persoonlijke, bedrijfs- of andere informatie, niet dan na uitdrukkelijke toestemming van de rechthebbende natuurlijke of rechtspersonen zal worden opgenomen, ge(re)presenteerd en/of gedistribueerd. De informatie zal uitsluitend worden gebruikt voor de doeleinden die de gebruikers ermee hebben beoogd. Onder 'persoonlijke informatie' wordt verstaan: alle informatie die direct of indirect herleidbaar is tot natuurlijke personen. Onder 'bedrijfsinformatie' wordt verstaan: alle informatie die betrekking heeft op bedrijven, instellingen of andersoortige organisaties. Onder 'andere informatie' wordt verstaan: alle informatie, die betrekking heeft of zou kunnen hebben op persoonlijke of bedrijfsinformatie. Daywize zal de in haar applicaties opgenomen informatie, van welke aard of inhoud dan ook, nooit aan derden verkopen, doen verkopen of anderszins beschikbaar (doen) stellen.

- **Statistische doeleinden**
  Daywize kan analyses uitvoeren voor statistische doeleinden. Voor zover Daywize de haar ter beschikking gestelde informatie gebruikt voor statistische doeleinden, wordt informatie te allen tijde gedepersonaliseerd en uitsluitend aangewend ten behoeve van de kwalitatieve verbetering van de door Daywize ontwikkelde applicaties en/of de verbetering van de kwaliteit van de service aan gebruikers.

- **Beveiliging gewaarborgd**
  Daywize verplicht zich tegenover haar gebruikers alles te doen wat redelijkerwijs in haar vermogen ligt om – met inzet van alle daartoe geëigende of benodigde middelen of methoden – te bewerkstelligen, dat misbruik van de in de door haar ontwikkelde applicaties opgenomen informatie door derden – met inbegrip van gebruikers of medewerkers van Daywize – wordt tegengegaan, voorkomen of verhinderd. Daywize verplicht zich de beveiliging van de gegevens van gebruikers te waarborgen.

4.2 Wet- en regelgeving

Met ingang van 1 januari 2016 is een wijziging van de Wet Bescherming Persoonsgegevens (WBP) in werking getreden die een meldplicht regelt voor datalekken. Deze meldplicht houdt in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken moeten melden aan de Autoriteit Persoonsgegevens, en in bepaalde gevallen ook aan de betrokkene. De betrokkene is degene van wie persoonsgegevens zijn gelekt.

Op 25 mei 2018 treedt een nieuwe Europese privacywet in werking, namelijk de General Data Protection Regulation (GDPR). Dit is een privacywetgeving die geldt binnen de hele EU. In Nederland is deze privacyverordening bekend onder de naam Algemene Verordening Gegevensbescherming. Deze regelgeving wordt in alle lokale privacywetten binnen de hele EU en Europese Economische Ruimte (EER) geïmplementeerd. De verordening geldt voor alle organisaties die producten of diensten verkopen aan burgers in Europa en hun persoonsgegevens verwerken, inclusief organisaties op andere continenten. De

verordening biedt burgers in de EU en EER meer controle over hun persoonsgegevens en moet waarborgen dat hun informatie goed wordt verwerkt. De nieuwe AVG vervangt de Wet Bescherming persoonsgegevens (Wbp).

De AVG maakt het noodzakelijk dat organisaties die persoonsgegevens van EU-burgers verwerken hun verwerkingsproces zodanig aanpassen dat deze in lijn is met de nieuwe privacyverordening. Dit houdt onder meer in dat de huidige bewerkersovereenkomst dient te worden omgezet naar een verwerkersovereenkomst die compliant is met de AVG. In het kader van deze wetgeving heeft Daywize haar bewerkersovereenkomst aangepast. De nieuwe Verwerkersovereenkomst inclusief het protocol dat Daywize hanteert in het geval van een datalek is toegevoegd in bijlage A.

De AVG stelt eisen aan de vorm en inhoud van afspraken tussen opdrachtgevers en leveranciers. Daarnaast stelt deze wet ook een aantal verplichtingen en beperkingen aan Daywize als verwerker. Op basis van de AVG zorgen wij ervoor dat:

- wij en onze leveranciers zich vanzelfsprekend aan de wet houden.
- het verwerken van persoonsgegevens alleen plaatsvindt op basis van schriftelijke instructies van onze opdrachtgevers (zoals uitgewerkt in de dienstverleningsovereenkomst) of de wet.
- de gegevensverstrekking aan derden voortvloeit uit de wet of het doel van de verwerking en geschiedt met specifieke toestemming van de opdrachtgever.
- er voldoende waarborgen zijn met betrekking tot technische en organisatorische beveiliging.
- gegevens die aan ons zijn toevertrouwd geheim worden gehouden.
- de werkgever als verwerkingsverantwoordelijke kan voldoen aan de meldplicht datalekken.
- bij het ontwikkelen van software het ‘privacy by design’ en ‘privacy by default’ principe wordt gehanteerd.
- er bindende verwerkersafspraken gemaakt worden met verwerkingsverantwoordelijken (jouw werkgever) en sub-verwerkers (onze leveranciers).

Wilt u weten wat wij doen aan privacy in het kader van de Algemene Verordening Gegevensbescherming? Lees dan onze Privacy Statement in bijlage B.

Bijlage A Verwerkersovereenkomst

Daywize BV, gevestigd aan de Krommewetering 61b te Utrecht (hierna: "**Verwerker**")

U doet als organisatie zaken met **Verwerker**. In het vervolg van deze overeenkomst wordt uw organisatie aangemerkt als "**Verwerkingsverantwoordelijke**".

De dienstverlening van Verwerker is gericht op het het ontwikkelen, implementeren en supporten van state-of-the-art HR software. Om deze diensten aan te kunnen bieden zal Verwerker Persoonsgegevens van sollicitanten, werknemers / zelfstandigen / vrijwilligers ("Medewerkers"), oud-medewerkers en/of uitkeringsgerechtigden verwerken. Uw organisatie zal daarbij optreden als Verwerkingsverantwoordelijke in de zin van de toepasselijke regelgeving en Verwerker. Deze Verwerkersovereenkomst bevat de voorwaarden waaronder u zal optreden als Verwerkingsverantwoordelijke en maakt onlosmakelijk onderdeel uit van de overeenkomst (hierna: "Hoofdovereenkomst") die u met ons heeft.

Nemen het volgende in aanmerking:

- Verwerkingsverantwoordelijke en Verwerker hebben een Hoofdovereenkomst gesloten voor het verrichten van e-HRM diensten door Verwerker aan Verwerkingsverantwoordelijke. Op grond hiervan verwerkt Verwerker in opdracht van Verwerkingsverantwoordelijke Persoonsgegevens. Deze Verwerkersovereenkomst maakt als bijlage onlosmakelijk deel uit van de Hoofdovereenkomst;

- Partijen zijn van mening dat Verwerkingsverantwoordelijke aangemerkt wordt als "Verwerkingsverantwoordelijke" in de zin van de Algemene Verordening Gegevensbescherming (hierna: "AVG") en dat Verwerker aangemerkt kan worden als "Verwerker" in de zin van de AVG met betrekking tot deze Persoonsgegevens;

- Verwerkingsverantwoordelijke stelt aan Verwerker Persoonsgegevens ter beschikking om ten behoeve van haar te verwerken. Verwerker is hiertoe bereid. Verwerkingsverantwoordelijke wijst de doeleinden en middelen aan voor de verwerking en waarvoor de hierin genoemde voorwaarden gelden. Verwerker is bereid de verplichtingen omtrent beveiliging en andere aspecten van de AVG na te komen, voor zover dit binnen zijn macht ligt.

- Partijen, mede gelet op het vereiste uit artikel 28 van de AVG, de opdracht tot en nadere afspraken omtrent de verwerking van persoonsgegevens door Verwerker ten behoeve van Verwerkingsverantwoordelijke schriftelijk wensen vast te leggen middels deze Verwerkersovereenkomst.

Verklaren te zijn overeengekomen als volgt:

Artikel 1. Doeleinden van verwerking

1.1 Verwerker verbindt zich onder de voorwaarden van deze Verwerkersovereenkomst in opdracht van Verwerkingsverantwoordelijke persoonsgegevens te verwerken. De toegestane verwerkingen worden door Verwerker uitgevoerd binnen een (semi-) geautomatiseerde omgeving.

1.2 Verwerker verwerkt de persoonsgegevens uitsluitend in overeenstemming met de schriftelijke verwerkingsinstructies die door de Verwerkingsverantwoordelijke zijn bekendgemaakt dan wel in overeenstemming met de verplichtingen voortvloeiend uit de Hoofdovereenkomst of deze Verwerkersovereenkomst. Verwerker zal de persoonsgegevens niet voor enig ander doel verwerken dan zoals door Verwerkingsverantwoordelijke is vastgesteld. Verwerkingsverantwoordelijke zal Verwerker op de hoogte stellen van de verwerkingsdoeleinden voor zover deze niet reeds in deze Verwerkersovereenkomst of de Hoofdovereenkomst zijn genoemd.

1.3 Verwerker heeft geen zeggenschap over het doel en de middelen voor de verwerking van persoonsgegevens. Verwerker neemt geen zelfstandige beslissingen over de ontvangst en het gebruik van de persoonsgegevens, de verstrekking aan derden en de duur van de opslag van persoonsgegevens.

1.4 Verwerkingsverantwoordelijke staat ervoor in dat zij een register zal bijhouden van de onder deze Verwerkersovereenkomst geregelde verwerkingen. Verwerkingsverantwoordelijke vrijwaart Verwerker tegen alle aanspraken en claims die verband houden met het niet of niet juist naleven van de meldingsplicht en/of registerplicht.

1.5 Verwerkingsverantwoordelijke staat er voor in dat de inhoud, het gebruik en de opdracht tot de verwerkingen van de persoonsgegevens zoals bedoeld in deze Verwerkersovereenkomst, niet onrechtmatig is en geen inbreuk maken op enig recht van derden.

1.6 Verwerker is louter verantwoordelijk voor de verwerking van de persoonsgegevens onder deze Verwerkersovereenkomst. Voor alle overige verwerkingen van persoonsgegevens, waaronder in ieder geval begrepen maar niet beperkt tot de verzameling van de persoonsgegevens door de Verwerkingsverantwoordelijke, verwerkingen voor doeleinden die niet door Verwerkingsverantwoordelijke aan Verwerker zijn gemeld, verwerkingen door derden en/of voor andere doeleinden, is Verwerker niet verantwoordelijk. De verantwoordelijkheid voor deze verwerkingen rust uitsluitend bij Verwerkingsverantwoordelijke.

Artikel 2. Verplichtingen Verwerker

2.1 Ten aanzien van de in artikel 1 genoemde verwerkingen zal Verwerker zorg dragen voor de naleving van de voorwaarden die, op grond van de AVG, worden gesteld aan het verwerken van persoonsgegevens door Verwerker vanuit diens rol.

2.2 Verwerker zal Verwerkingsverantwoordelijke, op diens verzoek daartoe en binnen een redelijke termijn, informeren over de door hem genomen maatregelen aangaande zijn verplichtingen onder deze Verwerkersovereenkomst.

2.3 De verplichtingen van de Verwerker die uit deze Verwerkersovereenkomst voortvloeien, gelden ook voor degenen die persoonsgegevens verwerken onder het gezag van Verwerker.

2.4 Het verwerken van persoonsgegevens door Verwerker zal nimmer met zich meebrengen dat de databases van Verwerker worden verrijkt met de gegevens afkomstig uit de datasets van Verwerkingsverantwoordelijke tenzij het de gegevens in geaggregeerde, niet herleidbare, vorm betreft voor het gebruik van gegevens voor facturatie en het doen van statisch onderzoek naar (de kwaliteit van) haar dienstverlening. In dat geval is het Verwerker toegestaan deze gegevens voor eigen overige doeleinden te gebruiken.

2.5 Verwerker zal de persoonsgegevens niet in een derde land buiten de Europese Economische Ruimte verwerken, zoals bedoeld in de AVG tenzij zij hier voorafgaand schriftelijke toestemming heeft ontvangen van Verwerkingsverantwoordelijke en/of dit gebeurd door een Sub-Verwerker die voorkomt op de lijst van gecertificeerde Privacy Shield organisaties.

Artikel 3. Sub-Verwerkers

3.1 Verwerker is niet bevoegd om de persoonsgegevens op enige wijze door Sub-Verwerkers te laten verwerken, anders dan als toegestaan ingevolge deze Verwerkersovereenkomst of de Hoofdovereenkomst, of met de voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke.

3.2 Niettegenstaande artikel 3.1 geeft Verwerkingsverantwoordelijke haar algemene toestemming dat Verwerker de in Bijlage 1 genoemde Sub-Verwerkers inschakelt voor het leveren van haar diensten. In het geval van een beoogde verandering inzake de toevoeging of vervanging van andere Sub-Verwerkers waarvoor de Verwerkingsverantwoordelijke een algemene toestemming geeft, licht Verwerker de Verwerkingsverantwoordelijke hierover vooraf in. Hierbij wordt de Verwerkingsverantwoordelijke de mogelijkheid wordt geboden om binnen 4 weken tegen deze verandering bezwaar te maken op basis van redelijke gronden. De volgende omstandigheden worden geacht, doch niet limitatief, redelijke gronden te zijn:

- de Verwerkingsverantwoordelijke kan aantonen dat het onwaarschijnlijk is dat de beoogde Sub-Verwerker kan voldoen aan de verplichtingen voortvloeiend uit deze verwerkersovereenkomst;
- De Verwerkingsverantwoordelijke kan aantonen dat het aannemelijk is dat het inschakelen of de vervanging van de beoogde andere Sub-Verwerker een onredelijk risico inhoudt voor de bescherming van persoonsgegevens;

Wanneer Verwerkingsverantwoordelijke bezwaar maakt tegen door de Verwerker ingeschakelde derden, zullen Partijen onderling in overleg treden om hiertoe tot een oplossing te komen.

3.3 Verwerker zorgt er in ieder geval voor dat deze derden schriftelijk dezelfde plichten op zich nemen als tussen Verwerkingsverantwoordelijke en Verwerker zijn overeengekomen. Verwerker staat in voor een correcte naleving van deze plichten door deze derden en is bij fouten van deze derden zelf jegens Verwerkingsverantwoordelijke aansprakelijk voor alle schade alsof hij zelf de fout(en) heeft begaan.

Artikel 4. Rechten van betrokkenen

4.1 In het geval dat een betrokkene een verzoek tot uitoefening van zijn/haar wettelijke rechten richt aan Verwerker, zal Verwerker het verzoek doorsturen aan Verwerkingsverantwoordelijke en de betrokkene hiervan op de hoogte stellen. Verwerkingsverantwoordelijke zal het verzoek vervolgens verder zelfstandig afhandelen. Indien blijkt dat de Verwerkingsverantwoordelijke hulp benodigd heeft van de Verwerker voor de uitvoering van een verzoek van een betrokkene, dan kan de Verwerker hiervoor kosten in rekening brengen.

Artikel 5. Beveiliging, geheimhouding en auditrecht

5.1 Verwerker spant zich in passende technische en organisatorische maatregelen te nemen met betrekking tot de te verrichten verwerkingen van persoonsgegevens, tegen verlies of tegen enige vorm van onrechtmatige verwerking (zoals onbevoegde kennisname, aantasting, wijziging of verstrekking van de persoonsgegevens). Verwerker heeft haar beveilingsmaatregelen verder gespecificeerd op www.daywize.nl/faq.

5.2 Verwerker spant zich in de beveiliging te laten voldoen aan een niveau dat, gelet op de stand van de techniek, de gevoeligheid van de persoonsgegevens en de aan het treffen van de beveiliging verbonden kosten, niet onredelijk is.

5.3 Op alle persoonsgegevens die Verwerker van Verwerkingsverantwoordelijke ontvangt en/of zelf verzamelt in het kader van deze Verwerkersovereenkomst, rust een geheimhoudingsplicht jegens derden. Verwerker zal deze informatie niet voor een ander doel gebruiken dan waarvoor hij deze heeft verkregen, tenzij deze in een vorm is gebracht dat deze niet tot betrokkenen herleidbaar is.

5.4 Deze geheimhoudingsplicht is niet van toepassing voor zover Verwerkingsverantwoordelijke uitdrukkelijke toestemming heeft gegeven om de informatie aan derden te verschaffen, indien het verstrekken van de informatie aan derden logischerwijs noodzakelijk is gezien de aard van de verstrekte opdracht en de uitvoering van deze Verwerkersovereenkomst, of indien er een wettelijke verplichting bestaat om de informatie aan een derde te verstrekken.

5.5 Verwerker is gerechtigd Verwerkingsverantwoordelijke toegangs- of identificatiecodes toe te wijzen. Verwerker is gerechtigd toegewezen toegangs- of identificatiecodes te wijzigen. Verwerker wijst Verwerkingsverantwoordelijke er op dat zij de toegangs- en identificatiecodes vertrouwelijk en met zorg hoort te behandelen en deze slechts op gepersonaliseerde wijze aan geautoriseerde personeelsleden kenbaar maakt. Verwerker is niet aansprakelijk voor schade of kosten die het gevolg zijn van gebruik of misbruik dat van toegangs- of identificatiecodes wordt gemaakt.

5.6 Verwerkingsverantwoordelijke heeft het recht om audits uit te laten voeren door een onafhankelijke ICT-deskundige die aan geheimhouding is gebonden ter controle van naleving van alle punten uit deze Verwerkersovereenkomst.

5.7 Deze audit vindt uitsluitend plaatst **nadat** Verwerkingsverantwoordelijke de bij Verwerker aanwezige soortgelijke auditrapportages heeft opgevraagd, beoordeeld en redelijke argumenten aanbrengt die een door Verwerkingsverantwoordelijke geïnitieerde audit alsnog rechtvaardigen. Een dergelijke audit wordt gerechtvaardigd wanneer de bij Verwerker aanwezige soortgelijke auditrapportages geen of onvoldoende uitsluitsel geven over het naleven van deze Verwerkersovereenkomst door Verwerker. De door Verwerkingsverantwoordelijke geïnitieerde audit vindt zes weken na voorafgaande aankondiging door Verwerkingsverantwoordelijke, en maximaal eens per jaar plaats.

5.8 Verwerker zal aan de audit meewerken en alle voor de audit redelijkerwijs relevante informatie, inclusief ondersteunende gegevens zoals systeemlogs, en medewerkers zo tijdig mogelijk en binnen een redelijke termijn, waarbij een termijn van maximaal vier weken redelijk is tenzij een spoedeisend belang zich hiertegen verzet, ter beschikking stellen. Verwerkingsverantwoordelijke zal er zorg voor dragen dat de audit een zo min mogelijk bedrijfsverstorend effect op de overige werkzaamheden van Verwerker veroorzaakt. De bevindingen naar aanleiding van de uitgevoerde audit zullen door Partijen in onderling overleg worden beoordeeld en, naar aanleiding daarvan, al dan niet worden doorgevoerd door één van de Partijen of door beide Partijen gezamenlijk.

5.9 De redelijke kosten voor de audit worden door de Verwerkingsverantwoordelijke gedragen, met dien verstande dat de kosten voor de in te huren derde altijd door Verwerkingsverantwoordelijke zullen worden gedragen.

5.10 Verwerker verplicht Sub-verwerkers periodiek een onafhankelijke IT-auditor of deskundige een onderzoek te laten uitvoeren ten aanzien van de organisatie van Sub-verwerker, teneinde te doen vaststellen dat Sub-verwerker aan het bepaalde in artikel 5.1 en 5.2 voldoet. Verwerker heeft het recht toe te (laten) zien op de naleving van de onder artikel 5.1 en 5.2 genoemde maatregelen. Daartoe stelt Sub-verwerker op verzoek van Verwerker onder geheimhouding een kopie van haar ISAE3402 en/of ISO27001 certificaat en/of eventueel toekomstige andere en algemeen geaccepteerde verklaringen en/of normenkader gebaseerd op nationale of internationale standaarden ter beschikking.

Artikel 6. Meldplicht

6.1 In het geval van een beveiligingslek en/of een datalek zoals bedoeld in artikel 33 AVG zal Verwerker, zich naar beste kunnen inspannen om Verwerkingsverantwoordelijke daarover onverwijld dan wel uiterlijk binnen achtenveertig (48) uur te infomeren naar aanleiding waarvan Verwerkingsverantwoordelijke beoordeelt of zij de toezichthoudende autoriteiten en/of betrokkenen zal informeren of niet. Verwerker spant zich naar beste kunnen in om de verstrekte informatie volledig, correct en accuraat te maken. De meldplicht geldt enkel indien het lek daadwerkelijk heeft plaatsgevonden. Zie bijlage 3 voor het Protocol datalekken Daywize.

6.2 Verwerkingsverantwoordelijke zal zorgdragen voor het voldoen aan eventuele (wettelijke) meldplichten. Indien de wet- en/of regelgeving dit vereist zal Verwerker meewerken aan het informeren van de ter zake relevante autoriteiten en eventueel betrokkenen, echter blijft de Verwerkingsverantwoordelijke de verantwoordelijke partij in het kader van deze wettelijke meldplicht.

6.3 De meldplicht behelst in ieder geval het melden van het feit dat er een lek is geweest, alsmede:

- de datum waarop het lek heeft plaatsgevonden (indien geen exacte datum bekend is: de periode waarbinnen het lek heeft plaatsgevonden;
- wat de (vermeende) oorzaak is van het lek;
- de datum en het tijdstip waarop het lek bekend is geworden bij Verwerker of bij een door hem ingeschakelde derde of onderaannemer;
- het aantal personen waarvan gegevens zijn gelekt (indien geen exact aantal bekend is: het minimale en maximale aantal personen waarvan gegevens zijn gelekt);
- een omschrijving van de groep personen van wie gegevens zijn gelekt, inclusief het soort of de soorten persoonsgegevens die gelekt zijn;
- of de gegevens versleuteld, gehasht of op een andere manier onbegrijpelijk of ontoegankelijk zijn gemaakt voor onbevoegden;
- wat de voorgenomen en/of reeds ondernomen maatregelen zijn om het lek te dichten en om de gevolgen van het lek te beperken;
- contactgegevens voor de opvolging van de melding.

Artikel 7. Aansprakelijkheid

7.1 Verwerker is jegens Verwerkingsverantwoordelijke als gevolg van of verband houdende met deze verwerkersovereenkomst of uit enige andere hoofde aansprakelijk voor zover en tot zover partijen dit zijn overeengekomen in de Hoofdovereenkomst. De in de Hoofdovereenkomst overeengekomen beperking van de aansprakelijkheid is onverminderd van kracht op de verplichtingen zoals opgenomen in deze Verwerkersovereenkomst, met dien verstande dat eenzelfde gebeurtenis nooit tot meerdere schadevorderingen kan leiden.

Artikel 8. Duur en beëindiging

8.1 Deze Verwerkersovereenkomst treedt in werking op 25 mei 2018 of, indien later, de datum van ondertekening door beide partijen en loopt qua duur gelijk aan de Hoofdovereenkomst. En in het geval bij het ontbreken van een Hoofdovereenkomst voor de duur van de samenwerking.

8.2 De Verwerkersovereenkomst kan tussentijds niet worden opgezegd.

8.3 Partijen mogen deze Verwerkersovereenkomst alleen wijzigen met wederzijdse schriftelijke instemming.

8.4 Na beëindiging van de Verwerkersovereenkomst zal Verwerker alle persoonsgegevens binnen een redelijke termijn terug overdragen aan Verwerkingsverantwoordelijke en/of op verzoek van Verwerkingsverantwoordelijke vernietigen of verwijderen, tenzij partijen anders overeenkomen en/of er een wettelijke plicht rust om te blijven verwerken.

Artikel 9. Overige bepalingen

9.1 De Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.

9.2 Alle geschillen, die tussen Partijen mochten ontstaan in verband met de Verwerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter in het arrondissement van de rechtbank die ook bevoegd is in het kader van de Overeenkomst te oordelen.

9.3 Indien één of meer bepalingen van de Verwerkersovereenkomst niet rechtsgeldig blijken te zijn, zal de Verwerkersovereenkomst voor het overige van kracht blijven. Partijen overleggen alsdan over de bepalingen welke niet rechtsgeldig zijn, teneinde een vervangende regeling te treffen die wel rechtsgeldig is en zoveel mogelijk aansluit bij de strekking van de te vervangen regeling.

9.4 Indien de privacywetgeving wijzigt, zullen partijen meewerken deze Verwerkersovereenkomst aan te passen teneinde aan deze wetgeving te kunnen (blijven) voldoen.

9.5 In geval van strijdigheid van verschillende documenten of de bijlagen daarvan, geldt de volgende rangorde:

a. deze Verwerkersovereenkomst;
b. de Hoofdovereenkomst;
c. de Algemene Voorwaarden van Verwerker;
d. eventuele aanvullende voorwaarden.

Door op akkoord te klikken gaat u akkoord met de inhoud van deze overeenkomst.

Bijlage 1: Specificatie Sub-verwerkers

Verwerker heeft toestemming van Verwerkingsverantwoordelijke om Sub-verwerkers in te zetten. Afhankelijk van de door Verwerkingsverantwoordelijke afgenomen diensten kunnen de volgende Sub-verwerkers van toepassing zijn:

Naam leverancier	Mendix Technology BV / XS4ALL, BIT, Dataplace, AWS (EU)
Korte omschrijving dienstverlening	Applicatieplatform / Hosting
Land van verwerking gegevens	Nederland en/of Europa
Relevante ISO-certificaten	ISAE3402 type 2 en ISO27001 / ISO27001

Naam leverancier	Nmbrs BV / **Uniserver Internet BV en anderen**
Korte omschrijving dienstverlening	Payroll / Hosting / overig
Land van verwerking gegevens	Nederland / Europa / Privacy Shield organisaties
Relevante ISO-certificaten	ISAE3402 type 2 / ISO27001

Naam leverancier	Sharebase BV
Korte omschrijving dienstverlening	Implementatie & Support Services / BPO / Procurement
Land van verwerking gegevens	Nederland en/of Europa
Relevante ISO-certificaten	Werken conform ISO 9001 processen Daywize BV

Naam leverancier	Talentsoft BV / Basefarm BV
Korte omschrijving dienstverlening	Applicant Tracking System / Hosting
Land van verwerking gegevens	Nederland
Relevante ISO-certificaten	ISAE3402 type 2 / ISO27001

Bijlage 2: Specificatie persoonsgegevens en betrokkenen

Persoonsgegevens

Bij het uitvoeren van de werkzaamheden, zoals aangeduid in de Hoofdovereenkomst, verwerkt de Verwerker persoonsgegevens. Afhankelijk van de door Verwerkingsverantwoordelijke afgenomen diensten kunnen de volgende (soort) persoonsgegevens worden verwerkt:

SOORT PERSOONSGEGEVENS [1]	N = risicoclassificering Normaal, H = risicoclassificering Hoog
• Naam-, adres- en woonplaatsgegevens (N) • Burgerservicenummer (H) • Contactgegevens zoals telefoonnummers en mailadressen (N) • Kopieën van legitimatiebewijzen (H) • Toegangs- of identificatiegegevens (N) • Bankrekeningnr. en financiële gegevens (N) • Aanstellings- / contractgegevens (N)	• Opleidingsgegevens (N) • Bezettings- en formatiegegevens (N) • Belonings-, uitkerings- en/of pensioengegevens en mutaties (N) • Verlofgegevens (N) • Verzuimgegevens (H) • Functioneringsgegevens (N) • Uitstroommutaties / uitdienstdata (N)
Overige persoonsgegevens, namelijk:	

Categorieën medewerkers

Afhankelijk van de door Verwerkingsverantwoordelijke afgenomen diensten kunnen de volgende (categorieën) medewerkers toegang hebben tot de persoonsgegevens:

- Volledige toegang vanwege beheer platform en applicatie-omgeving door system engineers, database administrators, application management support engineers
- Alleen lezen toegang vanwege oplossen van applicatie- en/of klantspecifieke incidenten door application developer en medewerkers service center
- Toegang tot klantspecifieke gegevens op projectbasis conform door Verwerkingsverantwoordelijke verleende autorisatie door implementatie-, product-, en/of conversiespecialisten.

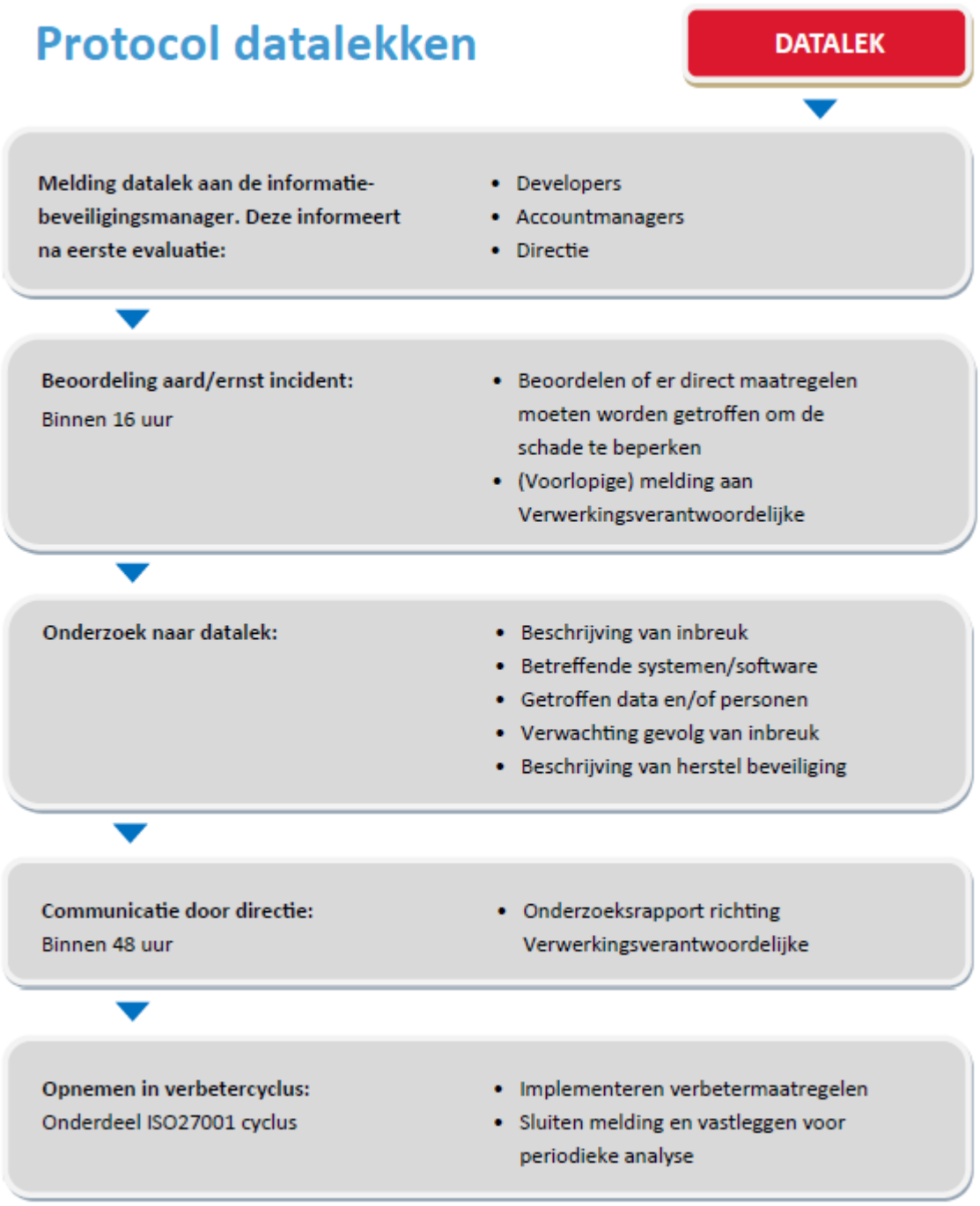
Categorieën betrokkenen

Afhankelijk van de door Verwerkingsverantwoordelijke afgenomen diensten kunnen de volgende persoonsgegevens van de volgende categorieën van betrokkenen worden verwerkt:

- Sollicitanten
- Werknemers / Zelfstandigen / Vrijwilligers (“Medewerkers”)
- Oud-medewerkers
- Uitkeringsgerechtigden

[1] Verwerkingsverantwoordelijke staat ervoor in dat de in deze bijlage omschreven persoonsgegevens volledig en correct zijn, en vrijwaart Verwerker voor enige gebreken en aanspraken die resulteren uit een incorrecte weergave.

Bijlage 3: protocol datalekken Daywize



Bijlage B Privacy Statement

Inleiding

Het onderstaande privacy beleid is van toepassing op alle sitebezoeken, transacties en overeenkomsten met Daywize. Wij respecteren de privacy van de bezoekers van onze website en/of de medewerkers van onze klanten (of de medewerkers van de klanten van onze partners). We dragen er zorg voor dat de persoonlijke informatie die je ons verschaft vertrouwelijk wordt behandeld. Hoe wij dit precies doen, en welke persoonsgegevens wij verzamelen voor welke doeleinden, kun je hieronder lezen.

Persoonsgegevens en waarvoor we deze gebruiken

Wij verwerken persoonsgegevens over jou doordat je gebruik maakt van onze website of interesse toont in onze diensten of reeds klant bent. Je kan hierbij denken aan:

- Voor- en achternaam
- Adresgegevens
- Geslacht
- Geboortedatum / Geboorteplaats
- Telefoonnummer / e-mailadres
- LinkedIn-adres
- Locatiegegevens
- Gegevens over jouw activiteiten op onze website
- Gegevens over jouw surfgedrag
- IP-adres, internetbrowser en apparaat type

Of overige persoonsgegevens die je actief verstrekt bijvoorbeeld door een profiel op onze website aan te maken, in correspondentie en telefonisch. Deze informatie gebruiken wij voor de volgende doelen:

- voor het verzenden van onze nieuwsbrief en/of reclamemailingen
- om je te kunnen bellen indien dit nodig is om onze dienstverlening uit te kunnen voeren
- om je te informeren over wijzigingen van onze diensten en producten
- om je de mogelijkheid te bieden een account aan te maken
- om diensten bij je af te leveren
- voor het afhandelen van betalingen

Daywize verwerkt ook persoonsgegevens als wij hier wettelijk toe verplicht zijn, zoals bijvoorbeeld gegevens die wij nodig hebben voor onze belastingaangifte.

Hoe lang we gegevens bewaren

Daywize zal je persoonsgegevens niet langer bewaren dan strikt nodig is om de doelen te realiseren waarvoor je gegevens worden verzameld.

Vertrouwelijkheid & verstrekking aan derden

Wij gaan vertrouwelijk met jouw persoonsgegevens om. De persoonsgegevens die wij via onze website verzamelen, verstrekken wij niet aan derde partijen voor direct marketing doeleinden van deze partijen. Verder zullen wij de door jouw verstrekte gegevens niet aan andere partijen verstrekken, tenzij je hier voorafgaande toestemming voor hebt verstrekt, dit noodzakelijk is in het kader van de uitvoering van de overeenkomst of wij dit op basis van de wet mogen of moeten doen.

Beveiliging

Daywize neemt de bescherming van jouw gegevens serieus en neemt passende maatregelen om misbruik, verlies, onbevoegde toegang, ongewenste openbaarmaking en ongeoorloofde wijziging tegen te gaan. Als jij het idee hebt dat jouw gegevens toch niet goed beveiligd zijn of er aanwijzingen zijn van misbruik, neem dan contact met ons op via info@daywize.nl.

In kaart brengen websitebezoek

Daywize gebruikt alleen technische en functionele cookies. En analytische cookies die geen inbreuk maken op je privacy. Een cookie is een klein tekstbestand dat bij het eerste bezoek aan deze website wordt opgeslagen op jouw computer, tablet of smartphone. De cookies die wij gebruiken zijn noodzakelijk voor de technische werking van de website en jouw gebruiksgemak. Ze zorgen ervoor dat de website naar behoren werkt en onthouden bijvoorbeeld jouw voorkeursinstellingen. Ook kunnen wij hiermee onze website optimaliseren. Je kunt je afmelden voor cookies door je internetbrowser zo in te stellen dat deze geen cookies meer opslaat. Daarnaast kun je ook alle informatie die eerder is opgeslagen via de instellingen van je browser verwijderen.

Gegevens inzien, aanpassen of verwijderen

Je hebt het recht om je persoonsgegevens in te zien, te corrigeren of te verwijderen. Je kunt een verzoek tot inzage, correctie of verwijdering sturen naar info@daywize.nl. Om er zeker van te zijn dat het verzoek tot inzage door jou is gedaan, vragen wij jou een kopie van je identiteitsbewijs bij het verzoek mee te sturen. Hierbij vragen we jou om in deze kopie je pasfoto, MRZ (machine readable zone, de strook met nummers onderaan het paspoort), paspoortnummer en burgerservicenummer (BSN) zwart te maken. Dit ter bescherming van je privacy. Daywize zal zo snel mogelijk, maar binnen vier weken, op jouw verzoek reageren.

Als we persoonsgegevens verwerken omdat je werkgever klant is

Wij kunnen ook persoonsgegevens over jou verwerken omdat je werkgever deze gegevens aan ons of aan een van onze partners heeft verstrekt. Wij hanteren verschillende maatregelen om je privacy als medewerker te waarborgen en jouw persoonsgegevens te beschermen. Onze verwerking van persoonsgegevens voldoet aan de Nederlandse en Europese privacywetgeving en -richtlijnen. De Algemene Verordening Gegevensbescherming (AVG) is de basis voor ons informatiebeveiligings-beleid. De AVG beschouwt Daywize als ‘verwerker’, omdat onze dienstverlening erop gericht is om

persoons-, salaris- en daaraan gerelateerde gegevens te verwerken voor jouw werkgever die als opdrachtgever in de wet als 'verwerkingsverantwoordelijke' geldt.

Dat betekent concreet dat als jij het idee hebt dat er meer gegevens over jou verwerkt worden dan jij noodzakelijk acht en/of gegevens niet goed beveiligd zijn en/of er aanwijzingen zijn van misbruik, je als eerste contact moet opnemen met je werkgever. Deze is volgens de wet namelijk hoofdverantwoordelijk. Wij verwerken enkel de gegevens op aangeven en instructie van jouw werkgever.

Afhankelijk van de door jouw werkgever afgenomen diensten kunnen wij de volgende soorten persoonsgegevens verwerken:

- Naam-, adres- en woonplaatsgegevens
- Burgerservicenummer
- Contactgegevens zoals telefoonnummers en mailadressen
- Kopieën van legitimatiebewijzen
- Toegangs- of identificatiegegevens
- Bankrekeningnr. en financiële gegevens
- Aanstellings- / contractgegevens
- Opleidingsgegevens
- Bezettings- en formatiegegevens
- Belonings-, uitkerings- en/of pensioengegevens en mutaties
- Verlofgegevens
- Verzuimgegevens
- Functioneringsgegevens
- Uitstroommutaties / uitdienstdata

De AVG stelt eisen aan de vorm en inhoud van afspraken tussen opdrachtgevers en leveranciers. Daarnaast stelt deze wet ook een aantal verplichtingen en beperkingen aan Daywize als verwerker. Op basis van de AVG zorgen wij ervoor dat:

- wij en onze leveranciers zich vanzelfsprekend aan de wet houden.
- het verwerken van persoonsgegevens alleen plaatsvindt op basis van schriftelijke instructies van onze opdrachtgevers (zoals uitgewerkt in de dienstverleningsovereenkomst) of de wet.
- de gegevensverstrekking aan derden voortvloeit uit de wet of het doel van de verwerking en geschiedt met specifieke toestemming van de opdrachtgever.
- er voldoende waarborgen zijn met betrekking tot technische en organisatorische beveiliging.
- gegevens die aan ons zijn toevertrouwd geheim worden gehouden.
- jouw werkgever als verwerkingsverantwoordelijke kan voldoen aan de meldplicht datalekken.
- bij het ontwikkelen van software het 'privacy by design' en 'privacy by default' principe wordt gehanteerd.
- er bindende verwerkersafspraken gemaakt worden met verwerkingsverantwoordelijken (jouw werkgever) en sub-verwerkers (onze leveranciers).

Bijlage C Waarom Daywize kiest voor Mendix

Daywize Cloud is ontwikkelt op het Mendix App Platform. Dit is een strategische keuze. Tegenwoordig is het belangrijk dat organisaties snel in kunnen spelen op veranderende (markt)omstandigheden. Om een specifiek probleem op te lossen of een kans in de markt te benutten zijn doorgaans nieuwe moderne, gebruiksvriendelijk applicaties nodig die makkelijk en snel in te zetten zijn.

In de praktijk blijkt echter vaak dat de huidige enterprise-architectuur innovatie in de weg staat. De afgelopen jaren hebben organisaties hard gewerkt om de architectuur op te bouwen volgens het traditionele vijflagenmodel (user interface, process, integratie, transactie en data). Deze gelaagde architectuur vormt het fundament van veel organisaties en maakt het mogelijk om op een heldere en gestructureerde manier naar alle aspecten van de architectuur te kijken en stelt CIO's onder andere in staat om de releasestrategie, het beheermodel en de data-integriteit te waarborgen.

Toch kleven er ook wat nadelen aan het huidige model, waardoor snelle applicatieontwikkeling geremd wordt. Zo kost het ontwikkelen van nieuwe applicaties binnen deze architectuur bijvoorbeeld veel tijd, is ontwikkelen middels de watervalmethode noodzakelijk en gaat het ontwikkelen van deze applicaties gepaard met forse investeringen. Er kan wel gesteld worden dat de huidige enterprise-architectuur te rigide is om op gewenste snelheid mee te kunnen. Toch is van de hand doen ook geen optie, dus de vraag rijst: hoe kan de enterprise-architectuur geflexibiliseerd worden?

Enterprise aPaaS rukt op

Als nieuwe applicaties niet onder architectuur ontwikkeld kunnen worden of door de business zelf als cloudapplicatie aangeschaft kunnen worden, moeten organisaties andere middelen aanwenden. Een opvallende ontwikkeling op dit gebied is de opkomst van het Enterprise Application Platform-as-a-service, ook wel Enterprise aPaas genoemd. De aPaas begint wereldwijd steeds meer voet aan de grond te krijgen. Met betrekking tot de ontwikkelaarservaring wordt ook wel de term High Productivity Platform gehanteerd. Dergelijke platformen worden aangeboden als cloud-service en stelt organisaties in staat om vanuit een centrale omgeving snel datagedreven applicaties te (laten) ontwerpen en implementeren voor iedere omgeving en device. Snelle applicatieontwikkeling wordt mogelijk gemaakt doordat het platform gebaseerd is op model driven development, bestaat uit open-source componenten en XML-gebaseerd is.

Snelheid op alle lagen

Het fenomeen High Productivity Platform is echter niet echt nieuw. Veel organisaties hebben al wel eens één of meerdere applicaties ontwikkeld op een dergelijk platform. Maar om de huidige enterprise-architectuur te flexibiliseren en klaar te zijn voor de toekomst is het zaak om het platform strategisch in te zetten en te migreren naar een vaste plek binnen de architectuur.

Juist een strategische inzet van binnen de huidige architectuur kan het verandervermogen van organisaties aanzienlijk vergroten, zonder de uitgangspunten met betrekking tot beheer uit het oog te verliezen. Het omarmen van een High Productivity Platform zorgt ervoor dat een totaal beheerplatform wordt neergezet, waar vanuit alle applicaties en de beveiliging hiervan centraal gemanaged kunnen worden. Een wildgroei aan losse applicaties buiten het zicht van IT wordt hierdoor voorkomen.

Doordat een High Productivity Platform meestal een best-of-suite oplossing is die alle lagen uit het vijflagenmodel in zich verenigt, kan op elke laag waarde worden toegevoegd. Zo kunnen bijvoorbeeld extra functionaliteiten aan bestaande bedrijfskritische applicaties worden toegevoegd. Denk bijvoorbeeld aan het geschikt maken van een applicatie voor mobiel gebruik of het aanpassen van de grafische interface. De levensduur van legacy-systemen kan hierdoor aanzienlijk verlengd worden en de gedane investeringen in applicaties kunnen zo verder worden uitgenut.

De afweging om wel of niet een High Productivity Platform op te nemen in de architectuur is eigenlijk overbodig wanneer de CIO de organisatie klaar wil maken voor de toekomst. Door een dergelijk platform in te zetten in de huidige enterprise-architectuur worden organisaties niet meer beperkt en zijn ze klaar voor de toekomst, waardoor betere resultaten behaald kunnen worden op het gebied van snelheid, wendbaarheid en time-to-market.

Daywize Cloud: de basis voor een moderne uniforme gebruikerservaring

De best practices in Daywize Cloud dekken meer dan 90% van elk gewenste HR functionaliteit standaard af. Echter omdat Daywize Cloud ontwikkelt is op het Mendix App Platform kunnen wij met toepassing van de SCRUM-methode desgewenst in een korte doorlooptijd de laatste 10% klantspecifiek ontwikkelen. Of als u kiest voor de hiervoor beschreven enterprise aPaas strategie ook andere (staf)processen op een uniforme wijze ontsluiten richting medewerkers en managers.

Meer weten?

Voor meer informatie over het Mendix App Platform en hoe de beveiliging binnen het Mendix App Platform georganiseerd is verwijzen we u naar de volgende whitepapers:

- Mendix App Platform
- Security for Cloud and On-Premises Deployment