De voordelen van Software-as-a-Service

Defacto

Wat is SaaS?

Software-as-a-Service, kortweg SaaS, is de verzamelnaam voor software die als online dienst wordt aangeboden. Dit geldt vandaag de dag voor veel software. Denk hierbij aan de online variant van Microsoft Office, HR-software en diverse platforms voor bedrijfscommunicatie. SaaS kenmerkt zich door schaalbaarheid en het feit dat er één versie is voor alle gebruikers. Doordat de software benaderd wordt via een webbrowser is de software daarnaast altijd en overal beschikbaar.

Het beheer ligt volledig bij de aanbieder en met één druk op de knop kunnen (beveiligings)updates en upgrades worden doorgevoerd, zodat de afnemer altijd over de laatste versie beschikt.

Waarom SaaS?

Met de keuze voor SaaS ontlast u de werkdruk in de organisatie en hebt u zekerheid dat er altijd de hoogste prioriteit wordt gegeven aan privacy, encryptie van gegevens en de toegang tot de software-applicaties.

Doordat de service en support bij SaaS-oplossingen bij Defacto ligt, zijn wij niet afhankelijk van toegang of beschikbaarheid van uw ICT-afdeling, maar kunnen er continu updates doorgevoerd worden.

SaaS zorgt er voor dat u altijd beschikt over de laatste versie van de software.

Certificeringen

Defacto

Waar we aan voldoen om echt SaaS te kunnen bieden

Software-as-a-Service is meer dan alleen een term. Het is een visie op hoe Defacto haar producten en diensten ziet. Defacto zorgt dat het aan alle relevante wet- en regelgeving voldoet op het gebied van certificering, privacy, softwaredesign en beleidsvoering, waaronder de Baseline Informatiebeveiliging Overheid (BIO).

De organisatie, diensten en software voldoen aan de ISO-certificeringen: ISO 9001, 14001, 27001, 27018, SOC2 Type I Attestation en NEN 7510.

Vanzelfsprekend zijn alle direct betrokken toeleveranciers van Defacto gecertificeerd voor de voor hen geldende certificeringen. Op verzoek kunnen de benodigde certificaten overlegd worden.

Kernpunten

Certificeringen:
ISO 9001, 14001, 27001, 27108 / NEN 7510 en SOC2 Type I Attestation

Voldoet aan:
AVG, BIO

Privacy:
Hoge standaarden worden aangehouden op gebied van dataminimalisatie (anonimisatie) en softwaretoegang (enkel toegang via versleuteld webverkeer en encryptieprotocollen TLS 1.2 en 1.3).

Bij versturen van data zoals resultaten en persoonsgegevens wordt dit waar nodig geanonimiseerd.

Privacy by design

Met deze manier van ontwikkelen zorgt Defacto dat er zowel technisch als organisatorisch zorgvuldig met persoonsgegevens wordt omgegaan en dat dit door interne processen ook gewaarborgd blijft. Bij de ontwikkeling van onze software wordt hier uitvoerig rekening mee gehouden. De werkwijze en producten van Defacto zijn dan ook volledig in overeenstemming met de richtlijnen op het gebied van de Algemene Verordening Gegevensbescherming (AVG).

Dataminimalisatie

Een voorbeeld van privacy by design is dataminimalisatie. Hiermee wordt bedoeld dat enkel de minimaal vereiste persoonsgegevens gebruikt worden, die strikt noodzakelijk zijn voor het verwerken van data. Waar mogelijk worden gegevens geanonimiseerd.

Beveiliging van data en toegang tot de software

Databeveiliging en de toegang tot de software en diensten van Defacto heeft de hoogste prioriteit en de Security Officer van de organisatie zorgt dat dit gewaarborgd blijft. Met betrekking tot onze applicaties wordt dit op de volgende wijze gerealiseerd:

- Toegang is slechts mogelijk via versleuteld webverkeer (HTTPS) en vertrouwde encryptie protocollen (TLS 1.2 en 1.3)
- Wachtwoorden worden slechts opgeslagen als een *one-way salted hash*
- Toegangslogs worden verzameld
- Wachtwoorden worden niet in logs opgeslagen
- Aanmaak wachtwoorden gebeurt door gebruikers zelf, bij verlies wordt deze aangepast aan de hand van een unieke link met tijdelijk bruikbaar token
- Er kan nooit ingelogd worden zonder wachtwoord of credentials via *Single-Sign-On* (SSO)
- *Single-Sign-On* is mogelijk via ADFS of OpenID

Beleid en controle

Defacto

Organisatiebeleid databeveiliging Defacto

Defacto heeft een Security Officer voor de waarborging van de correcte afhandeling en omgang waar het gaat om databeveiliging, security protocollen en certificeringen. Daarnaast werkt Defacto samen met een externe partij die actief kwetsbaarheden opspoort en rapporteert.

Intern beleid

Elke medewerker ondertekent de Defacto Security Checklist. Deze bevat best practices en eisen waar alle medewerkers aan moeten voldoen. Denk hierbij aan:

- Versleutelen van alle data en altijd vergrendelen van alle apparatuur
- Verplicht gebruik wachtwoordmanager met gegenereerde wachtwoorden
- Two Factor Authenticatie (2FA) verplicht (waar mogelijk)
- Clean desk policy (nooit onbeschermd laten van vertrouwelijke gegevens)
- Meldingsplicht van informatiebeveiligingsincidenten
- Toegang tot data en services is need-to-know op basis van functie
- Kennis van de meest voorkomende kwetsbaarheden (OWASP)

Alle medewerkers nemen zes keer per jaar verplicht deel aan intern geörganiseerde security workshops.

Kernpunten

Intern beleid
Security Officer van Defacto waarborgt de interne informatieveiligheid, controle van toegang tot en omgang met data.

Medewerkers blijven jaarlijks actief betrokken bij het voldoen aan beleid op gebied van informatieveiligheid.

Externe controle:
Samenwerking met externe partij (‘Controleur’) voor:

Opsporen kwetsbaarheden, het verantwoord melden hiervan en het structureel scannen van de applicaties met automatische en real-time rapportage.

Externe controle

Defacto werkt samen met een onafhankelijke, externe partij voor het continu beveiligen en monitoren van onze applicaties:

1. Pentests via Research Programs
Via Research Programs worden ethische hackers (‘Researchers’) ingezet om onbekende kwetsbaarheden in onze applicaties op te sporen. Voor al onze applicaties bestaat een testomgeving waar continue pentests plaatsvinden. Wanneer een kwetsbaarheid wordt gevonden, word Defacto automatisch en realtime geïnformeerd over de aard en ernst van de kwetsbaarheid.

2. Responsible disclosure
Responsible disclosure staat voor het op verantwoorde manier melden van kwetsbaarheden, middels een daarvoor opengesteld kanaal. Via Controleur faciliteert Defacto het verantwoord rapporteren van kwetsbaarheden.

3. Wekelijkse Automatische Scanners
Controleur biedt op eenvoudige wijze de beste kwetsbaarheden-scanners aan om de veiligheid van onze applicaties te monitoren. Deze scanners draaien wekelijks op onze omgevingen en onze developers ontvangen hier direct de rapporten van, zodat dagelijks veranderende kwetsbaarheden zo snel mogelijk herkend kunnen worden.

Continuïteit

Defacto

Data-integriteit

Behalve het belang van dataveiligheid en toegang tot de software, is het ook essentieel dat de integriteit van de data bewaakt wordt. Om deze reden vindt er een gecontroleerde systeem- en data back-up plaats. Back-ups worden 30 dagen bewaard. Hierover kunnen, indien gewenst, aanvullende afspraken worden gemaakt.

Back-up en datarecovery

Alle CAPP LMS-applicaties zijn op databaseniveau uitgerust met just-in-time recovery. Dit houdt in dat de toestand van een database teruggezet kan worden naar een willekeurig te kiezen tijdstip dat in het verleden ligt. Deze recovery heeft een bereik van 7 dagen. Verder hanteren we een *disaster recovery* van maximaal vier uur en bieden mutatielogs inzicht in eerder gedane wijzigingen in de data.

Alle dataopslag is redundant uitgevoerd. Op verzoek kan Defacto een snapshot of data-dump maken van een database en deze opleveren, in een gangbaar formaat (thans SQL- of CSV-formaat).

Kernpunten

Back-up en datarecovery
Back-ups worden maximaal 30 dagen bewaard. Aanvullende afspraken zijn mogelijk.

CAPP LMS:
Data kan binnen een bereik van 7 dagen naar elk willekeurig moment teruggezet worden.

Continuïteit:
Defacto stelt kosteloos een continuïteitsregeling beschikbaar als alternatief voor een zogeheten kostbare Escrow-regeling.

Waarborging Continuïteit

Defacto stelt kosteloos een continuïteitsregeling beschikbaar als alternatief voor een zogeheten kostbare Escrow-regeling voor data met onderstaande eigenschappen:

- In geval van calamiteiten aangaande de continuïteit van Defacto waarborgt Defacto de volledige voortgezette toegang voor een bepaalde periode voor alle gebruikers met passende gebruiksrechten als mede de aan Afnemer toebehorende data door:
- Een financiële garantstelling bij onafhankelijke derde die contractueel garandeert dat de hosting van de diensten voor in ieder geval een periode van zes maanden na het intreden van de calamiteit zullen worden voortgezet. Deze continuïteitsgarantie is schriftelijk overeengekomen;
- Op verzoek periodiek een back-up van de databases beschikbaar te stellen via een beveiligde service, onder de voorwaarde dat Afnemer deze back-up enkel gebruikt in geval van insolventie van Defacto;
- De mogelijkheid voor Afnemer om gedurende de looptijd van de overeenkomst haar data te exporteren en zelf op te slaan.

Beheer

Defacto

Support in het geval van on-premise

In de on-premise situatie is Defacto slechts gedeeltelijk in staat tot het leveren van kwalitatieve support. Dit wegens het gebrek aan toegang tot de eigen applicatie en de bijbehorende infrastructuur. Deze situatie vereist de aanwezigheid op locatie van onze technische consultants.

Support in het geval van SaaS

In het geval van SaaS wordt er verbeterde support geleverd doordat:

- Defacto toegang heeft tot de applicatie wanneer nodig.
- Er sneller onderzoek kan worden verricht met daarbij horende actie.
- Communicatie rechtstreeks tussen u en Defacto verloopt.

Responsetijden liggen tijdens kantooruren onder de 10 minuten.

Kernpunten

On-premise:
Beperkte toegang en respons snelheid mogelijk.

SaaS:
Directe toegang, hoge respons snelheid en snelle communicatie mogelijk.

Technisch beheer:
Server uptime van **99,99% (24/7)**.
In geval van SaaS is tussenkomst van (externe) ICT-dienstverlener niet meer van toepassing.

Functioneel beheer:
SaaS stelt Defacto in staat om sneller te reageren en te schakelen met onze klanten.

Technisch beheer

Defacto is verantwoordelijk voor het up-to-date houden van haar software en bijbehorende hardware samen met de hiervoor door Defacto geselecteerde leveranciers. Defacto garandeert een beschikbaarheid van 99%, gemeten tijdens kantooruren per 12 kalendermaanden. Problemen met beschikbaarheid die worden veroorzaakt door de internetprovider van eindgebruikers vallen buiten de verantwoordelijkheid van Defacto. Onze huidige uptime ligt op 99,99% (24/7).

Eventuele errors en problemen (zowel binnen de applicatie als op hosting niveau) worden real-time automatisch gesignaleerd via e-mail, sms en onze interne chatapplicaties. Hiermee kan Defacto direct acteren op eventuele problemen en zorgen dat de software snel weer in de lucht is.

Functioneel beheer

Dit blijft zoals het on-premise ook is. Wel is Functioneel Beheer minder afhankelijk van trage responsetijden en lage prioriteitstelling van eigen systeembeheer. Ons Support Team schakelt in de regel direct met Functioneel Beheer van onze klanten en kan hierdoor snel inspelen op situaties.

Software

Defacto

Up-to-date software

SaaS-oplossingen zijn altijd in beheer van de leverancier. Deze is dan ook verantwoordelijk voor upgrades en updates. Als afnemer hoeft u daarom nooit patches te downloaden, installeren, of extra hardware aan te schaffen. Bovendien werkt u altijd met de nieuwste versie van de software. In de praktijk betekent dit dat updates geruisloos uitgevoerd worden, zodat de eindgebruikers er niets van merken.

Upgrades van de software

Defacto ontwikkelt volgen een strikte test-driven development aanpak. Dit betekent dat vóór het toepassen van veranderingen op de applicatie eerst automatische tests worden opgesteld. Deze aanpak zorgt er daarmee ook voor dat eventuele onverwachte bijeffecten van de veranderingen vrijwel altijd worden ondervangen door eerder geschreven automatische tests.

Tijdens de ontwikkeling van software hanteert Defacto een workflow waarbij veranderingen eerst lokaal in een ontwikkelomgeving worden ontwikkeld en vervolgens zonder downtime geïmplementeerd worden. In de praktijk betekent het dat kleine verbeteringen voor de gebruikerservaringen, het oplossen van bugs en security verbeteringen op elk moment kunnen worden doorgevoerd waardoor de vereiste werkzaamheden van uw ICT-afdeling duidelijk zullen verminderen.

Kernpunten

Up-to-date software:
SaaS-oplossingen verminderen werklast klant, altijd up-to-date.

Upgrades van de software:
Upgrades van CAPP LMS zijn continu, geen beperkt aantal releases per jaar.

SaaS als trend en kostenreductie:
Minimaliseert overheadkosten op ICT-gebied.

Gebruiker

Defacto

Anyplace, anywhere, anytime

SaaS-oplossingen zijn op elk moment beschikbaar vanaf elk apparaat met toegang tot het internet - dus niet alleen vanaf het intranet. Bovendien is iedereen tegenwoordig vertrouwd met het internet, én met het gebruik van SaaS-oplossingen (denk bijvoorbeeld aan Gmail, Netflix, iCloud en Dropbox). Daarom hebben SaaS-oplossingen meestal een hogere acceptatiegraad en een lagere leercurve.

Performance

Met de keuze voor een SaaS-oplossing kiest u voor optimale performance. Zo is het eenvoudig om de resources van datacenters automatisch op te schalen wanneer er sprake is van toegenomen gebruik en af te schalen wanneer dit weer afneemt. Hierdoor zullen gebruikers op individueel niveau geen last ondervinden wanneer er sprake is van toegenomen dataverkeer. Verder biedt SaaS de medewerker de mogelijkheid om altijd en overal toegang te krijgen tot het systeem.

Kernpunten

Gebruiker centraal:
SaaS-oplossingen worden positiever door gebruikers ervaren dan on-premise.

Performance:
Organisaties zijn niet afhankelijk van de interne infrastructuur en met SaaS-oplossingen wordt er automatisch ingespeeld op toe- en afname in dataverkeer.

Meer informatie

Indien u eens met ons in gesprek wilt over onze SaaS-oplossingen, meer informatie wilt over hoe dit bij uw organisaties geïmplementeerd kan worden of andere vragen hebt, dan kunnen we u in contact brengen met onze accountmanagers en technisch consultants die u hier graag mee van dienst zijn.

Zuiderpark 3, 9724 AD, Groningen | 050 3144832 | info@defacto.nl