Producten en Diensten dormakaba Nederland

In deze bijlage zijn de producten van dormakaba Nederland, diensten van dormakaba Nederland en de specifieke toelichtingen die daarbij horen opgenomen. dormakaba Nederland kan deze bijlage van tijd tot tijd wijzigen als er andere producten worden aangeboden of als deze uit haar assortiment verdwijnen.

I. Producten urenmanagement

A. Time-Wize

B. Time-Wize Experience

C. Time-Wize Saphir

D. Eagle

E. Argos

Consultancy voor de inrichting van Urenmanagement

Voor de inrichting van de applicatie biedt dormakaba Nederland consultancy aan. Deze consultancy kan op locatie bij de klant worden uitgevoerd of desgewenst op kantoor bij dormakaba Nederland. De specifieke consultancy zorgt ervoor dat het product wordt ingericht volgens de scope waarin de opdrachtgever de regelgeving en de instellingen heeft gedefinieerd. Dat kan een CAO, bedrijfsregeling of individuele regeling zijn.

Nadere toelichting Producten urenmanagement en Consultancy voor de inrichting van Urenmanagement

De software kan on-premise worden geïnstalleerd of beschikbaar zijn als SaaS (Online platform). Deze software kan worden ingezet voor alle branches waarbij de basisfunctionaliteit de registratie en verdere berekening van gewerkte uren van medewerkers/uitzendkrachten/inleners is. Deze gewerkte uren kunnen worden verbijzonderd: op kostenplaats/product/werkorder. Bij het gebruik van de module toegangsbeheer kunnen medewerkers worden geautoriseerd om ergens wel of niet naar binnen te mogen (terrein, pand, afdeling). Er kunnen diverse interfaces worden ingesteld naar HRM- en ERP applicaties. Vanuit de ESS (Employee Self Service) en Management Self Service (MSS) functionaliteit kunnen medewerkers afwezigheden aanvragen en leidinggevenden (Management Self Service) hebben inzage in de bezetting op een afdeling om op basis daarvan verlofaanvragen te accorderen. De smartphone, tablet en laptop kunnen gebruikt worden voor ESS-gebruik.

Aanvullend geldt voor product A t/m C:
Met de smartphone kan een medewerker “klokken”, afwezigheden opgeven en heeft de medewerker inzicht in zijn/haar kloktijden.

** De voor deze Verwerkersovereenkomst van toepassing zijnde producten en/of diensten staan vermeld in de door dormakaba Nederland uitgebrachte offerte*

II. ReQuest

ReQuest: building solutions

I. Toegangscontrole

   Hiermee kunnen medewerkers en bezoekers worden geautoriseerd om ergens wel of niet naar binnen te mogen.

II. Digitaal Knoppenpaneel

Het digitaal knoppenpaneel geeft een overview van een site waarbij het mogelijk is om de status te zien van toegangen en deze op afstand te sturen en is het eenvoudig te zien waar er meldingen zijn.

III. Contractor Management

Contractors kunnen vooraf aangemeld worden voor een bezoek aan uw bedrijf en op deze manier voor een bepaalde periode of bepaalde tijden toegang krijgen tot een locatie.

IV. Tijdregistratie – Self Service Terminal

Het registeren van werktijden per medewerker of project.

Aanwezigheidsregistratie
Op ieder moment is hiermee inzicht te krijgen wie er op een locatie, in een pand of een afdeling aanwezig zijn.

Lockermanagement
Aansturen en uitgave van lockers aan personeelsleden en bezoekers.

ReQuest: Veiligheid

a) Dynamisch gebouwgebruik
Geeft in een overzicht aan welke werkplekken er beschikbaar zijn in een pand.

b) Incident management
Applicatie waarbij meldingen vanuit de overige systemen kunnen leiden tot een melding in het systeem. De opvolging van het incident wordt daarbij direct in de applicatie vastgelegd.

c) Kunstbeveiliging
Door middel van het detecteren van bewegingen kunnen kunstobjecten beveiligd worden.

d) Asset Tracking
Hiermee kunnen goederen gevolgd worden op gebruik of aanwezigheid of ter controle of deze zich op de juiste plek bevinden.

Bezoekersregistratie

a) Kubiq Guest
Hiermee kunnen bezoekers aangemeld worden voor een bezoek aan uw bedrijf. Deze aanmelding kan zowel voor- als achteraf plaatsvinden, waarbij de bezoeker zichzelf vooraf aan kan melden.

BHV-management

a) KubiQ Guard

Real-time inzicht in het aantal beschikbare hulpverleners per locatie. Met de KubiQ Guard app op de smartphone kunnen de hulpverleners direct geïnformeerd en geïnstrueerd worden tijdens een incident vanuit één centraal punt, waarbij alle informatie wordt vastgelegd.

Voor alle toepassingen geldt dat er interfaces ingesteld kunnen worden naar bijvoorbeeld HRM- en ERP applicaties, verschillende soorten Security Management Systemen of Facilitair Management Informatie Systemen.

Consultancy voor de inrichting van ReQuest

Voor de inrichting van de applicatie biedt dormakaba Nederland consultancy aan. Deze consultancy kan op locatie bij de klant worden uitgevoerd of desgewenst op kantoor bij dormakaba Nederland. De specifieke consultancy zorgt ervoor dat het product wordt ingericht volgens de scope waarin de eindgebruiker de instellingen heeft gedefinieerd.

Nadere toelichting

Voor Building Solutions en Veiligheid kan de software voor ReQuest on premise worden geïnstalleerd of beschikbaar zijn als SaaS. Deze software kan worden ingezet voor alle branches en voor al de omschreven dormakaba-oplossingen.

** De voor deze Verwerkersovereenkomst van toepassing zijnde producten en/of diensten staan vermeld in de door dormakaba Nederland uitgebrachte offerte.*

III. Exos

User management

Met deze module wordt bepaald welke medewerker één of meerdere van de onderstaande functionaliteiten kan inzien en beheren. De rol binnen de software is één van de belangrijkste functies om te bepalen welke modules en dus welke (persoons) gegevens moeten kunnen worden ingezien in het systeem. De module user management is standaard in het systeem aanwezig.

Toegangscontrole

Binnen het Exos systeem richten we de hardware functioneel in en bepalen daarin de volledige werking van het systeem. Hier zijn onder andere de toegangsprofielen, tijdzones en alle specifieke modules zoals onderstaand beschreven in opgenomen.

Personenbeheer

Binnen het toegangssysteem beheren we personen en daarbij de volgende minimaal noodzakelijke gegevens:

- Pasnummer
- Personeelsnummer
- Naam – eventueel geanonimiseerd
- Toegangsprofiel(en)
- Veel gegevens zijn optioneel vast te leggen, maar hangen af van de technische/ functionele werking van het systeem in zijn geheel en de gebruikte module.

Bezoekersbeheer

Binnen de module bezoekersbeheer worden bezoekers vastgelegd indien deze onderdeel moeten zijn van het toegangssysteem. Bezoekers worden vooraf of bij aankomst in het toegangssysteem ingevoerd. Minimaal de volgende gegevens zijn noodzakelijk:

- Bezoekersnaam
- Pasnummer
- Toegangsprofiel
- Gastheer uit interne organisatie

Contractorbeheer

Binnen de module contractorbeheer worden contractors vastgelegd indien deze onderdeel moeten zijn van het toegangssysteem. Bezoekers worden vooraf of bij aankomst in het toegangssysteem ingevoerd. Minimaal de volgende gegevens zijn noodzakelijk:

- Naam contractor medewerker en bedrijf
- Pasnummer
- Toegangsprofiel Optioneel kunnen aanwezige uren worden geregistreerd en kunnen hiervan rapportages voor controle van aanwezige uren worden gemaakt.

Alarmbeheer

De module alarmbeheer is een generieke functie die voor elk project op maat wordt ingericht. De eindgebruiker bepaald zelf wat als alarm moet worden gedefinieerd. Dit kan een relatie hebben met persoonsgegevens indien het alarm persoon gerelateerd is. Het pasnummer en de naam van de persoon zal dan tezamen met het alarm worden getoond. Bijvoorbeeld indien een toegangskaart wordt aangeboden bij een lezer waar dit niet mag op basis van het toegangsprofiel.

Ruimtebeheer en aanwezigheidsoverzicht

Met deze module wordt via boekingen bij kaartlezers bijgehouden waar een persoon zich in het gebouw of op het terrein bevindt. Deze functie heeft een relatie met de overzichtsschermen voor aanwezigheid, processen voor ontruimingen en veiligheidsprocessen voor wat betreft IN/UIT controle, anti-passback.

Logboeken

Binnen de logboeken wordt vastgelegd welke acties er binnen het systeem plaatsvinden. Het onderstaande wordt in elke systeem als standaard gebruikt:

- Audit logboek, legt alle wijzigingen binnen de software vast, incl. persoonsgegevens (naam) van de beheerder
- Toegangslogboek, legt alle boekingen van personen bij deuren vast in het systeem
- Alarmlogboek, legt alle alarmen binnen het systeem vast, incl. eventueel persoonsgegevens indien het alarm een persoon betreft

Alle logboeken hebben een instelbare bewaartermijn van de gegevens.

Badge-printen en personaliseren

Met deze module kunnen gepersonaliseerde toegangskaarten worden gemaakt, waardoor de gebruiker herkenbaar is in de organisatie. Alle gegevens uit het toegangssysteem, incl. pasfoto kunnen hiervoor gebruikt worden. De eindgebruiker bepaalt zelf het nut- en de noodzaak hiervan.

Foto-vergelijk

Deze securityfeature geeft de mogelijkheid om een controle uit te voeren op het gebruik van toegangskaarten. Een securitymedewerker vergelijkt bij een boeking bij een kaartlezer de foto uit de database met het live-beeld van een camera bij het toegangspunt. Hiervoor zal in het toegangssysteem dus minimaal de naam en een pasfoto moeten zijn opgeslagen.

Beheer mechanische sleutels/Depot-control

Betreft de uitgifte en registratie hiervan in het systeem waarbij minimale persoonsgegevens nodig zijn. Handmatige uitgifte of via geautomatiseerde sleutel-depot systemen zullen worden opgenomen in de logboeken en onderdeel kunnen zijn van het alarmbeheer indien sleutels niet tijdig zijn geretourneerd. Optioneel kan een sleuteluitgifte formulier worden gebruikt voor registratie en akkoordverklaring op papier.

Lockermanagement

Met deze module worden vanuit het toegangsbeheersysteem de rechten en het gebruik daarvan in lockers beheerd. Het is integraal onderdeel van het toegangsbeheer en de registratie in logboeken.

Individuele berichtgeving

Een optionele module om aan gebruikers (pashouders) binnen het systeem berichten te kunnen versturen. Hiervoor zijn naast de minimaal noodzakelijke persoonsgegevens ook het Emailadres van de gebruiker nodig.

Parkeerbeheer

Met deze module wordt de toegang tot een parkeerterrein georganiseerd en worden ook alle toegangsboekingen van het in-/uitrijden in het toegangslogboek en parkeerlogboek vastgelegd.

Mobile Access
Met deze module is het mogelijk om toegang te verlenen aan medewerkers, bezoekers en/of contractors met behulp van een smartphone. Aanvullend op de minimaal noodzakelijke persoonsgegevens geldt dat het telefoonnummer van de gebruiker noodzakelijk is.

Interfaces:

- LDAP/ Active directory
- API
- SAP /ERP
- Alle interface zullen afzonderlijk moeten worden beoordeeld voor wat betreft de noodzakelijke gegevens die met het toegangssysteem gedeeld worden. Dit is maatwerk en hangt af van de gewenste functionaliteit binnen het systeem.

Het bovenliggende systeem is altijd leidend voor wat betreft toevoegen, wijzigen of verwijderen van gegevens en ook voor welke gegevens er precies in het toegangssysteem worden geplaatst.

Consultancy voor de inrichting van Exos

Voor de inrichting van de applicatie biedt dormakaba Nederland consultancy aan. Deze consultancy kan op locatie bij de klant worden uitgevoerd of desgewenst op kantoor bij dormakaba Nederland. De specifieke consultancy zorgt ervoor dat het product wordt ingericht volgens de scope waarin de opdrachtgever de regelgeving en de instellingen heeft gedefinieerd. We kunnen tevens AVG-advies geven over de inrichting van de applicatie. Dit heeft betrekking op de afhankelijkheden van het systeem en hoe die qua opzet aan de AVG kan voldoen.

Nadere toelichting

De software kan on-premise worden geïnstalleerd of beschikbaar zijn als SaaS (Online platform). Bij het gebruik van de module toegangsbeheer kunnen medewerkers worden geautoriseerd om ergens wel of niet naar binnen te mogen (terrein, pand, afdeling). Er kunnen diverse interfaces worden ingesteld naar HRM- en ERP applicaties. Vanuit de ESS (Employee Self Service) functionaliteit kunnen medewerkers eigen gegevens raadplegen en bezoekers uitnodigen.

** De voor deze Verwerkersovereenkomst van toepassing zijnde producten en/of diensten staan vermeld in de door dormakaba Nederland uitgebrachte offerte.*

IV. Matrix

User management

Met deze module wordt bepaald welke medewerker één of meerdere van de onderstaande functionaliteiten kan inzien en beheren. De rol binnen de software is één van de belangrijkste functies om te bepalen welke modules en dus welke (persoons) gegevens moeten kunnen worden ingezien in het systeem. De module user management is standaard in het systeem aanwezig.

Toegangscontrole

Binnen het Exos systeem richten we de hardware functioneel in en bepalen daarin de volledige werking van het systeem. Hier zijn onder andere de toegangsprofielen, tijdzones en alle specifieke modules zoals onderstaand beschreven in opgenomen.

Personenbeheer

Binnen het toegangssysteem beheren we personen en daarbij de volgende minimaal noodzakelijke gegevens:

- Pasnummer
- Personeelsnummer
- Naam – eventueel geanonimiseerd

- Toegangsprofiel(en)
- Veel gegevens zijn optioneel vast te leggen, maar hangen af van de technische/ functionele werking van het systeem in zijn geheel en de gebruikte module.

Bezoekersbeheer

Binnen de module bezoekersbeheer worden bezoekers vastgelegd indien deze onderdeel moeten zijn van het toegangssysteem. Bezoekers worden vooraf of bij aankomst in het toegangssysteem ingevoerd. Hierbij zijn minimaal de volgende gegevens noodzakelijk:

- Bezoekersnaam
- Pasnummer
- Toegangsprofiel
- Gastheer uit interne organisatie

Contractorbeheer

Binnen de module contractorbeheer worden contractors vastgelegd indien deze onderdeel moeten zijn van het toegangssysteem. Contractors worden vooraf of bij aankomst in het toegangssysteem ingevoerd. Hierbij zijn minimaal de volgende gegevens noodzakelijk:

- Naam contractor medewerker en bedrijf
- Pasnummer
- Toegangsprofiel Optioneel kunnen aanwezige uren worden geregistreerd en kunnen hiervan rapportages voor controle van aanwezige uren worden gemaakt.

Alarmbeheer

De module alarmbeheer is een generieke functie die voor elk project op maat wordt ingericht. De eindgebruiker bepaald zelf wat als alarm moet worden gedefinieerd. Dit kan een relatie hebben met persoonsgegevens indien het alarm persoon gerelateerd is. Het pasnummer en de naam van de persoon zal dan tezamen met het alarm worden getoond. Bijvoorbeeld indien een toegangskaart wordt aangeboden bij een lezer waar dit niet mag op basis van het toegangsprofiel.

Ruimtebeheer en aanwezigheidsoverzicht

Met deze module wordt via boekingen bij kaartlezers bijgehouden waar een persoon zich in het gebouw of op het terrein bevindt. Deze functie heeft een relatie met de overzichtsschermen voor aanwezigheid, processen voor ontruimingen en veiligheidsprocessen voor wat betreft IN/UIT controle, anti-passback.

Bewakingsronde

Deze module wordt gebruikt tijdens een ronde die de bewaking loopt/rijdt over een terrein. Alle boekingen en tijd die ertussen zit wordt gecontroleerd. Bij afwijkingen op de gestelde parameters zal een alarm gegeneerd worden.

Tijdregistratie

Deze module wordt gebruikt om overzicht te genereren van de aanwezigheid en de berekening van aanwezige uren voor medewerkers en/of contractors.

Logboeken

Binnen de logboeken wordt vastgelegd welke acties er binnen het systeem plaatsvinden. Het onderstaande wordt in elke systeem als standaard gebruikt:

- Audit logboek, legt alle wijzigingen binnen de software vast, incl. persoonsgegevens (naam) van de beheerder
- Toegangslogboek, legt alle boekingen van personen bij deuren vast in het systeem
- Alarmlogboek, legt alle alarmen binnen het systeem vast, incl. eventueel persoonsgegevens indien het alarm een persoon betreft

Alle logboeken hebben een instelbare bewaartermijn van de gegevens.

Badge-printen en personaliseren

Met deze module kunnen gepersonaliseerde toegangskaarten worden gemaakt, waardoor de gebruiker herkenbaar is in de organisatie. Alle gegevens uit het toegangssysteem, incl. pasfoto kunnen hiervoor gebruikt worden, en eindgebruiker bepaalt nut- en noodzaak hiervan zelf.

Foto-vergelijk

Deze securityfeature geeft de mogelijkheid om een controle uit te voeren op het gebruik van toegangskaarten. Een securitymedewerker vergelijkt bij een boeking bij een kaartlezer de foto uit de database met het live-beeld van een camera bij het toegangspunt. Hiervoor zal in het toegangssysteem dus minimaal de naam en een pasfoto moeten zijn opgeslagen.

Documentimport

Met deze module is het mogelijk om bij de persoon ook bestanden op te slaan, zoals bijvoorbeeld ondertekende veiligheidsinstructies of certificaten. Bij het verwijderen van een persoon zullen ook deze documenten verwijderd worden.

Mobile Access

Interfaces:

- Integration management
- API
- SAP /ERP

Consultancy voor de inrichting van Matrix

Voor de inrichting van de applicatie biedt dormakaba Nederland consultancy aan. Deze consultancy kan op locatie bij de klant worden uitgevoerd of desgewenst op kantoor bij dormakaba Nederland. De specifieke consultancy zorgt ervoor dat het product wordt ingericht volgens de scope waarin de opdrachtgever de regelgeving en de instellingen heeft gedefinieerd. We kunnen tevens AVG-advies geven over de inrichting van de applicatie. Dit heeft betrekking op de afhankelijkheden van het systeem en hoe die qua opzet aam de AVG kan voldoen.

Nadere toelichting

De software kan on-premise worden geïnstalleerd of beschikbaar zijn als SaaS (Online platform). Bij het gebruik van de module toegangsbeheer kunnen medewerkers worden geautoriseerd om ergens wel of niet naar binnen te mogen (terrein, pand, afdeling). Er kunnen diverse interfaces worden ingesteld naar HRM- en ERP applicaties. Vanuit de ESS (Employee Self Service) functionaliteit kunnen medewerkers eigen gegevens raadplegen en bezoekers uitnodigen.

** De voor deze Verwerkersovereenkomst van toepassing zijnde producten en/of diensten staan vermeld in de door dormakaba Nederland uitgebrachte offerte.*

V. Privacy by Design

dormakaba Nederland heeft bij het ontwerpen van haar product *Privacy by Design* het navolgende in overweging genomen:

Gegevens van medewerkers

Het uitgangspunt is dat er standaard zo min mogelijk (Persoons)gegevens van medewerkers (Data subject) worden vastgelegd die nodig zijn voor het registeren en verantwoorden van uren. Indien voor de juiste berekeningen en werking van het toegangssysteem aanvullende gegevens van een medewerker vastgelegd dienen te worden, dan is het mogelijk deze af te schermen en via een autorisaties in te stellen wie daartoe wel de mogelijkheid heeft om deze (Persoons)gegevens in te zien.

Aanvullend geldt voor Urenmanagement:

In overleg met de Opdrachtgever wordt bepaald welke gegevens vastgelegd dienen te worden. In de (tijd-/toegang) terminals wordt naast eventueel een naam van de medewerker, geen aanvullende gegevens van medewerkers vastgelegd waarbij in een toegangsterminal ook geen naam van de medewerker wordt gekoppeld. Deze autorisatie gebeurt op basis van een uniek criterium waarbij er een referentie is met betrekking tot de geheugenlocatie en de medewerker.

Aanvullend geldt voor Urenmanagement (Eagle & Argos):

De rechten in de stamgegevens zijn af te schermen, waardoor alleen geautoriseerde gebruikers toegang hebben tot deze gegevens. Het is door de geïntegreerde opzet mogelijk dat de toegang tot de stamgegevens aan/uit kunnen worden gezet in de profielen. Het is niet mogelijk om alleen bepaalde stamgegevens/tabs open te zetten. Toegang tot de stamgegevens betekent toegang tot alle stamgegevens.

Data beveiliging

Uren management (Time-Wize, Time-Wize Experience & Time-Wize Saphir):

Bij data-export wordt gebruik gemaakt van de back-up tool Time-Wize databasemanager. Hierbij worden de gegevens standaard geanonimiseerd en encrypted met een zelf te bepalen wachtwoord. Hiermee is het mogelijk om niet op de fysieke locatie van de Opdrachtgever de verdere configuratie te realiseren en eventuele probleemanalyses uit te voeren.

Bij het Online platform (SaaS) is het volgende relevant om te vermelden:

- Standaard wordt SSL toegepast (Dataverbinding encryptie)
- Toepassing van Transparent Data Encryption (TDE[1]) - encrypts SQL Server
- Standaard 2 factor authentication (Toekomstig voor Saphir)
- Passwordpolicy dat wil zeggen verplicht wachtwoordcomplexiteit en wachtwoord wijzigen na maximaal 90 dagen.

dormakaba Nederland levert een standaard applicatie die klant specifiek wordt ingericht. Op het moment dat een Opdrachtgever een issue meldt over de werking van de softwareapplicatie dan kan dormakaba Nederland een back-up opvragen om een situatie bij haar op kantoor te simuleren. dormakaba Nederland maakt gebruik van een volledig nieuwe manier om een dump aan te leveren. Deze supporttool - Time-Wize databasemanager - is speciaal ontwikkeld naar aanleiding van de bepalingen uit de AVG. De functionaliteiten waar Time-Wize databasemanager over beschikt, zorgen ervoor dat het aan de nieuwe regels wat betreft dataminimalisatie voldoet. Met Time-Wize databasemanager wordt een dump (back-up) van de gegevens uit Time-Wize gemaakt. In Time-Wize databasemanager worden de gegevens van de medewerkers automatisch geanonimiseerd, bepaalde gegevens worden niet getoond of het wordt zo ingevuld dat er niet na te gaan is over wie de informatie gaat.

De medewerkers zijn hierbij alleen nog te herkennen aan een uniek nummer. De gegevens worden hierbij samengevoegd in één bestand dat vervolgens wordt opgeslagen en versleuteld met een door de Opdrachtgever gekozen wachtwoord. Zonder wachtwoord van Opdrachtgever kan dormakaba Nederland de dump niet gebruiken. Deze dump wordt samen met het password via de dormakaba Nederland Supportsite verstuurd. Na ontvangst kan de consultant van dormakaba Nederland op basis van deze dump en de beschreven probleemstelling van de Opdrachtgever aan de slag. Dat betekent dat terugkoppeling van de oplossing door de consultant gebeurt op basis van het unieke nummer of de fictieve naam die aan de persoon is gekoppeld. Als een Opdrachtgever gebruik maakt van het Online platform (SaaS) waarbij de data is geplaatst bij onze outsourcing partij/ Subverwerker Cloudleverancier, dan zal dormakaba Nederland voor het simuleren van een issue dezelfde procedure volgen als hierboven beschreven.

[1] * Wat is TDE?
TDE voert real-time I/O-codering en decodering van de gegevens en logbestanden uit.
De codering gebruikt een databasecoderingssleutel (DEK), die in het opstartrecord van de database wordt opgeslagen voor beschikbaarheid tijdens herstel. De DEK is een symmetrische sleutel die is beveiligd door een certificaat te gebruiken dat is opgeslagen in de hoofddatabase van de server of door een asymmetrische sleutel die wordt beschermd door een EKM-module. TDE beschermt gegevens "in rust", dat wil zeggen de gegevens en logbestanden. TDE biedt de mogelijkheid om te voldoen aan vele wetten, voorschriften en richtlijnen die in verschillende industrieën zijn vastgesteld.

Urenmanagement (Eagle & Argos):

dormakaba Nederland levert een standaard applicatie die op de Opdrachtgever/Verwerkingsverantwoordelijke specifiek wordt ingericht. Bij een data-export worden de gegevens waar mogelijk geanonimiseerd. Hiermee is het mogelijk om Hiermee is het mogelijk om niet op de fysieke locatie van de Opdrachtgever de verdere configuratie te realiseren en eventuele probleemanalyses uit te voeren. Als Opdrachtgever/Verwerkingsverantwoordelijke gebruik maakt van het Online Platform (SaaS) waarbij de data is geplaatst bij onze outsourcingpartner (Cloudleverancier), dan zal dormakaba Nederland voor het simuleren van een issue dezelfde procedure volgen als hierboven beschreven.

Het volgende is relevant om te vermelden:

- Binnen de SaaS-omgeving wordt SSL/ HTTPS toegepast. Als de software bij de klant zelf draait ligt de verantwoordelijkheid hiervan bij de klant/beheerder van de server.
- Slechts een beperkt aantal medewerkers heeft toegang tot de SaaS-omgeving op server niveau.
- Er worden dagelijks (off-site) back-ups gemaakt van alle klantdata.