VOOR UW FG EN IT

Wat uw FG en IT willen weten

Voor uw functionaris gegevensbescherming en uw IT-beheerder: hoe de server beveiligd is, welke verbindingen hij maakt, wie wat mag zien en wat u zelf controleert. De beveiliging en de rechten op deze pagina zijn ingericht en getest; bij de eerste levering controleren wij ze op de echte server.

Bijgewerkt op 29 oktober 2026

AANMELDEN

Tweede factor verplicht

standaard, voor iedereen

SCHIJF

Versleuteld

met uw sleutel

BEHEERTOEGANG

Met uw toestemming

hooguit 24 uur

VAN BUITEN

Geen open poort

Beveiliging

Hoe de server beveiligd is

De server staat bij u op kantoor en is standaard zo ingericht:

- Iedereen meldt zich aan met een wachtwoord en een tweede factor, een code uit een app. Dat is standaard verplicht.
- De schijf met uw gegevens is versleuteld (LUKS). De sleutel is van u; wij hebben hem niet.
- Beheer op afstand kan alleen nadat een beheerder bij u op kantoor de toegang heeft opengezet, voor hooguit 24 uur.
- Elke beheersessie en elke inzage komt in een logboek op uw server, dat u zelf kunt lezen en exporteren.

Tweede factor verplicht · Versleutelde schijf (LUKS) · Logboek bij u

Verwachtingen

Wat u van ons kunt verwachten

Wat de dienst in de praktijk betekent:

- Wij controleren uw server 24/7, met een kort statusbericht elk kwartier. Ziet de controle een probleem, dan nemen wij contact met u op.
- Hulp van een mens: op werkdagen van 9:00 tot 17:00, met een reactie binnen 4 werkuren.
- Vragen en antwoorden gebeuren op de server in uw kantoor, niet via internet.
- Na een stroomstoring start de server zelf weer op en ontgrendelt hij de schijf, zolang de sleuteldienst in uw netwerk bereikbaar is.
- Gaat er iets mis, dan zetten wij samen met u de back-up van de afgelopen nacht terug. U verliest hooguit de wijzigingen sinds die back-up; gesprekken zitten niet in de back-up.

Controle 24/7 · Reactie binnen 4 werkuren · Hooguit één dag aan wijzigingen

Back-ups

Back-ups, gescheiden van de server

De back-up staat niet op de server zelf:

- Elke nacht gaat een versleutelde back-up van uw documenten, instellingen en logboek naar aparte opslag bij u op kantoor, bijvoorbeeld uw NAS. De laatste 14 blijven staan.
- Alleen uw sleutel opent hem; wij hebben die sleutel niet en bewaren geen kopie.
- Bij de oplevering doen we samen een hersteltest. Wij raden aan die elk kwartaal te herhalen.
- Een back-up buiten uw kantoor kan erbij, tegen meerprijs.

Elke nacht, 14 versies · Buiten kantoor: tegen meerprijs

Verbindingen

Welke verbindingen de server maakt

Van buiten naar binnen: geen, er staat geen poort open. Naar buiten maakt de server alleen deze verbindingen:

- korte statusberichten voor de 24/7 controle, zonder namen, bestanden of inhoud;
- de beheerverbinding, versleuteld, en alleen terwijl uw beheerder de toegang heeft opengezet;
- software-updates, alleen in het afgesproken onderhoudsvenster;
- de gewone diensten voor naamopzoeking (DNS) en de tijd.

Naar binnen: niets · Nooit documenttekst naar buiten

Accounts

Accounts en rechten

Wie wat mag zien, regelt u zelf:

- De accounts staan op uw eigen server. Uw beheerder maakt ze aan en trekt ze in.
- Rechten gelden per dossier. Een medewerker is eigenaar, bewerker of lezer van een dossier, of heeft er geen toegang toe.
- Elke medewerker heeft een persoonlijk dossier dat alleen hij of zij ziet.
- Het Arcanto-model gebruikt alleen dossiers die de gebruiker zelf mag lezen.

Accounts op uw server · Rechten per dossier

Uitvoer

De uitvoer controleert u zelf

Het Arcanto-model vat samen, stelt op en beantwoordt vragen uit uw documenten. Bij elk antwoord staat waar het vandaan komt: het document en de passage, met een verwijzing als [1] of [2]. Het kan zich vergissen. Wat eruit komt, controleert een medewerker in het stuk zelf voordat het wordt gebruikt. AI-uitvoer is geen geverifieerd advies; de verantwoordelijkheid voor het werk blijft bij uw kantoor.

Bron bij elk antwoord · Een mens controleert

Logboeken

Wat er wordt vastgelegd

Drie logboeken, op uw eigen server:

- Het toegangslogboek: per dossier wie zocht, wie een document opende, en wie een dossier maakte, de leden of de vaste instructie wijzigde. Persoonlijke dossiers staan er niet in. Uw beheerder ziet het in de werkplek.
- Het logboek van beheer: elke beheersessie, elk verzoek om inzage en elke toestemming. U leest en exporteert het zelf.
- Het gebruikslogboek: per vraag de medewerker en het tijdstip, niet de vraag zelf.

Wie wat opende · Elke beheersessie

Onderzoek

Beveiliging laten onderzoeken

Wij hebben de beveiliging van de software zelf getest. Wilt u haar ook laten onderzoeken, door uw eigen IT-partij of een onafhankelijke partij, dan kan dat op de geïnstalleerde server, in overleg.

In overleg, op uw server

Koppelingen

Koppelingen met uw kantoorsoftware

Een koppeling met uw dossiersysteem (DMS) of EPD is mogelijk, op aanvraag.

DMS of EPD: op aanvraag

Stukken

Beveiligingspakket en verwerkersovereenkomst

Het volledige beveiligingspakket ontvangt u op aanvraag; de verwerkersovereenkomst bij de offerte.

Op aanvraag

De vragen die uw FG en IT stellen

Zijn de documenten ook op de server zelf versleuteld?

Ja. De schijf met uw gegevens is versleuteld (LUKS), met uw sleutel. Terwijl de server draait, is de schijf ontgrendeld; daarom hoort de server in een afsluitbare ruimte of kast.

Zijn er een tweede factor, persoonlijke accounts en rechten per rol?

Ja. Iedereen heeft een eigen account met een tweede factor, standaard verplicht. Rechten gelden per dossier: eigenaar, bewerker of lezer.

Kunnen wij de beveiliging zelf laten onderzoeken?

Ja. Wij hebben de beveiliging van de software zelf getest. U kunt haar ook laten onderzoeken door uw eigen IT-partij of een onafhankelijke partij, op de geïnstalleerde server, in overleg.

Hoe gaat u om met updates, kwetsbaarheden en incidenten?

Updates installeren wij maandelijks in een afgesproken onderhoudsvenster. Een urgente beveiligingsupdate voeren we direct uit, na uw toestemming. Een inbreuk waarvan wij kennis krijgen, melden wij u uiterlijk binnen 24 uur na ontdekking.

Staan de back-ups apart van de server?

Ja. Elke nacht gaat een versleutelde back-up naar aparte opslag bij u op kantoor, bijvoorbeeld uw NAS. De laatste 14 blijven staan. Een back-up buiten uw kantoor kan erbij, tegen meerprijs.

Wanneer wordt het herstel getest?

Bij de oplevering doen we samen een hersteltest. Wij raden aan die elk kwartaal te herhalen.

Hoeveel gegevens kunnen we verliezen, en hoe snel is het hersteld?

Bij herstel uit de back-up verliest u hooguit de wijzigingen sinds de laatste nachtelijke back-up; gesprekken zitten er niet in. Een herstel uit de back-up doen we samen met u, zodra de hardware werkt. Is er hardware kapot, dan loopt de vervanging via de leverancier.

Wat gebeurt er als Arcanto langere tijd niet bereikbaar is?

Geplande afwezigheid van meer dan twee werkdagen melden wij minstens 14 dagen vooraf. De server heeft ons voor het dagelijkse werk niet nodig: vragen en antwoorden gebeuren op de server in uw kantoor, en uw back-ups staan bij u.

Kunnen wij de verwerkersovereenkomst vooraf beoordelen?

Ja. U ontvangt haar bij de offerte, vóór u tekent, samen met het beveiligingspakket.

Welke gegevens en logboeken worden verwerkt?

Op uw server: uw documenten, de gesprekken (zolang de bewaartermijn loopt), het gebruikslogboek, het toegangslogboek en het logboek van beheer. Naar ons gaan alleen statusberichten zonder namen, bestanden of inhoud.

Hoe worden verzoeken, verwijdering en datalekken afgehandeld?

Verzoeken van betrokkenen handelt u af op uw eigen server; komt er een bij ons binnen, dan sturen wij die naar u door. Gesprekken worden na de bewaartermijn gewist, documenten verwijdert u zelf. Een inbreuk melden wij uiterlijk binnen 24 uur na ontdekking.

Helpt u bij onze DPIA en interne audit?

Ja. Wij leveren de beschrijving van de dienst, de beveiligingsmaatregelen en het dreigingsmodel van de server. U mag eenmaal per jaar een controle laten uitvoeren.

Staat bij elk antwoord de bron?

Ja. Elk antwoord verwijst met [1], [2] naar het document en de passage waar het vandaan komt.

Hoe worden dossiers tussen medewerkers afgeschermd?

Per dossier is een medewerker eigenaar, bewerker of lezer, of heeft geen toegang. Persoonlijke dossiers ziet alleen de medewerker zelf. Het model gebruikt alleen dossiers die de vragensteller mag lezen.

Welke bestanden kan het lezen, en hoeveel gebruikers kan het aan?

Pdf, Word (docx), Excel (xlsx), csv en tekstbestanden. Hoeveel mensen tegelijk werken, bepaalt de opzet van uw server; dat stemmen we in het gesprek af op uw kantoor.

Kunnen wij het testen met eigen stukken?

Wij laten het zien in een gesprek, ook met uw eigen geanonimiseerde stukken.