Privacy statement 4Insurance

Inleiding

Dit Privacy Statement beschrijft van welke privacy strategie 4Insurance -en de aan haar gelieerde ondernemingen: AWI B.V. en Differ Solutions B.V. - gebruik maakt. We raden u aan om dit Privacy Statement aandachtig door te nemen.

4Insurance B.V. , AWI B.V. , Differ Solutions B.V.
Keesomstraat 16-1
6716 AB EDE
Info@awisoftware.nl

Uitgangspunt

In de Algemene Verordening Gegevensbescherming (AVG), en aanvullend in de overige relevante wet- en regelgeving met betrekking tot privacybescherming, zijn regels gesteld over de wijze waarop persoonsgegevens moeten worden verwerkt. 4insurance doet al het mogelijke om de privacy van haar klanten, relaties, gebruikers en overige betrokkenen te beschermen. Wij verwerken dan ook alleen die persoonsgegevens, die voor het aanbieden, het inrichten en het onderhouden van onze producten en diensten noodzakelijk zijn.

Begrippen

- **Persoonsgegevens:**
  Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene").
- **Verwerken:**
  Alles wat er met persoonsgegevens kan worden gedaan, zoals het verzamelen, het opslaan, het gebruiken en het verwijderen van persoonsgegevens uit onze administratie.
- **Verwerkingsverantwoordelijke:**
  De partij die alleen of samen met anderen, het doel van, en de middelen voor, de verwerking van persoonsgegevens vaststelt.
- **Verwerker:**
  De partij, die de gegevens verwerkt ten behoeve van de verwerkingsverantwoordelijke.

Verwerken van de persoonsgegevens

4Insurance biedt het volgende aanbod van producten en diensten:

- AWI Connect
- Eindklantenportals
- Sluitstraten en op maat gemaakte portals
- Dossiermanagementsystemen
- Fleet-/ lease applicaties
- Hosting van applicaties en data

De volgende categorieën van persoonsgegevens kunnen met betrekking tot de relaties, contactpersonen en gebruikers tenminste verwerkt worden bij het aanbod van de producten en diensten van 4Insurance:

- Voor- en achternamen, emailadres, telefoon;
- Geslacht;
- ID-nummer en het ID-kopiebewijs;
- Bankgegevens;
- Burgerlijke staat;
- Gezinssamenstelling;
- Leeftijd;
- Inkomen;
- Gebruiksnaam en wachtwoord.

Gegevens van relaties en contactpersonen worden verwerkt in diverse documenten zoals: Offertes, Contracten/Polissen, Orders, Facturen, en Correspondentie met de klant. Deze informatie wordt middels interfaces met onder andere (niet limitatief); Fish, FRISS, UBO opgehaald ter controle op integriteit, betrouwbaarheid en volledigheid.
Afhankelijk van de klantbehoeften kunnen ook persoonsgegevens over bijvoorbeeld de gezondheid worden verwerkt. Hiervoor is een juridische grondslag nodig, zoals het voldoen aan de toestemmingsvereiste.

4Insurance vervult zowel de rol van verwerkingsverantwoordelijke als die van verwerker.
In relatie met haar opdrachtgevers en klanten vervult zij de rol van verwerker.

Privacy statement 4Insurance

4Insurance maakt ook gebruik van derden (subverwerkers), waaraan zij werkzaamheden binnen het kader van haar dienstverlening uitbesteedt.

Rechtmatig handelen

4Insurance handelt zowel naar haar werknemers als naar haar opdrachtgevers/klanten en naar haar subverwerkers in overeenstemming met de AVG en de overige relevante wet- en regelgeving met betrekking tot de privacybescherming. Indien nodig wordt toestemming gevraagd aan betrokkenen voor de verwerking van de persoonsgegevens.

Bewaartermijnen

Persoonsgegevens worden bewaard in overeenstemming met de wettelijke bewaartermijnen, of, indien afwezig, in overeenstemming met de doeleinden, waarvoor de persoonsgegevens verwerkt worden.

Persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is.

Informatiebeveiliging

4Insurance heeft privacybescherming en informatiebeveiliging hoog in het vaandel staan. Daarvoor is 4Insurance zowel ISO27001 als ook ISO9001 gecertificeerd.
Onderstaand volgen maatregelen die 4Insurance onder andere getroffen heeft om haar gegevens te beveiligen. De maatregelen bestaan uit organisatorische en technische maatregelen.

A) Organisatorische maatregelen

1. Onze medewerkers krijgen alléén toegang tot de persoonsgegevens die ze nodig hebben voor het vervullen van hun functie.
2. Voor het verkrijgen van toegang tot persoonsgegevens zijn meerdere (onafhankelijke) lagen van beveiliging toegepast. Een aantal voorbeelden van die maatregelen zijn:
    a. Multi-factor (≥2) authentication
    b. Het gebruik van VPN t.b.v. versleuteling van netwerkverkeer.
3. Persoonsgegevens mogen in ons bedrijf nooit op andere plekken opgeslagen worden dan afgesproken. Hiervoor zijn interne procedures opgesteld.
4. Onze medewerkers hebben een geheimhoudingsverklaring getekend.
5. We maken gebruik van een password managementsysteem. Hiermee kunnen we een beveiligingsbeleid m.b.t het gebruik van wachtwoord-gebaseerde accounts aan onze medewerkers opleggen en controleren.
6. Medewerkers hebben een eigen laptop. Deze apparatuur wordt nooit met anderen gedeeld.
7. We zorgen ervoor dat medewerkers die ons bedrijf verlaten geen toegang meer hebben tot gegevens.
8. De software die we gebruiken voor het aanbieden van onze diensten voldoet aan de eisen in de wet.
9. Het bewustzijn bij medewerkers betreffende veilig werken wordt gestimuleerd, zoals het vragen van aandacht voor het niet openen van verdachte e-mails, het niet klikken op verdachte links, bij het langdurig verlaten werkplek uitloggen. De AVG is een periodiek terugkerend onderwerp in interne kennissessies.
10. Het bewaren van zaken achter slot en grendel (anders dan digitaal).
11. We hanteren een clean desk policy.
12. Rechten en rollen: vastgelegd is wie wat mag inzien, bijv. op bepaalde plekken op de schijf waar o.a. medewerker info wordt vastgelegd.

B) Technische maatregelen

1) Versleuteling: Bepaalde bestanden van diverse applicaties worden versleuteld opgeslagen.
2) Multi-factor (≥2) authentication waar nodig.
3) Toegangsbeveiliging: Voor toegang in de door 4Insurance geleverde systemen is een inlognaam en wachtwoord vereist. Deze kunnen op elk gewenst moment gewijzigd worden.
4) Autorisatie: Binnen de geleverde systemen wordt autorisatie uitgebreid toegepast, zodat alléén bevoegden gegevens in kunnen zien.
5) Gegevens minimalisatie: Wordt in combinatie met autorisatie uitgebreid toegepast.
6) Pseudonimisering of anonimisering van persoonsgegevens.
7) Server apparatuur staat in een speciale ruimte welke geconditioneerd en secure is.

Privacy by Design en Privacy by Default worden toegepast bij de ontwikkeling van nieuwe producten en diensten.

Omdat doorgaans de software van 4Insurance wordt geïnstalleerd in de omgeving van de verwerkersverantwoordelijke bij de AWI subverwerker, is deze ook indirect verantwoordelijk voor de beveiliging van deze omgeving.

C) Informatie over de door ons gebruikte datacenters via Webwizz (subverwerker)

Wij laten voor ons onze servers en overige apparatuur uitsluitend plaatsen in de meeste moderne datacenters. Deze datacenters bieden voor ons de juiste beveiliging tegen inbraak, brand, stroomuitval en overige calamiteiten. Deze datacenters hebben de onderstaande maatregelen genomen om te voldoen aan deze eisen en zijn ISO gecertificeerd. Ook de hosting partner is ISO gecertificeerd.

Voor apparatuur suites in het datacenter geldt:

1. Deze hebben voor de toevoer van elektriciteit naar onze apparatuur gescheiden feeds. Elke feed heeft op zijn beurt een eigen UPS-systeem.
2. De door ons gebruikte elektriciteit feeds hebben ruim voldoende overcapaciteit.
3. Elektriciteitstoevoer wordt gegarandeerd door het gebruik van UPS-systemen en noodstroomaggregaten. Voor langdurige verstoringen in het elektriciteitsnetwerk zijn leveringsafspraken voor het aanvullen van de brandstof voor deze noodstroomaggregaten aanwezig
4. Apparatuur is geplaatst op verhoogde datavloeren.
5. De datacenters beschikken over redundant uitgeruste klimaatbeheersing.
6. Er zijn voldoende maatregelen aanwezig om fysieke inbraak tot deze locaties te voorkomen of vertragen. Een aantal voorbeelden hiervan zijn:
    a. Beveiligd hekwerk
    b. Gravelbakken
    c. Extra verdikte muren
7. Deze datacenters beschikken over geavanceerde branddetectie- en blussystemen.
8. De datacenters zijn 24 uur per dag toegankelijk voor onze medewerkers onder strikte security regelgeving.
9. Ons apparatuur staat in afgesloten racks.
10. We maken uitsluitende gebruik van Nederlandse datacenters.
11. Er is permanente camerabewaking.

Er zijn strikte aanmeldprocedures om toegang te krijgen:

1. Alleen personen die op de vooraf aangelegde toegangslijst staan hebben toegang.
2. Bij binnenkomst wordt de identiteit van de bezoeker gecontroleerd door vakbekwaam beveiligingspersoneel.
3. Er gelden strikte aanmeldprocedures voor werkbezoeken.

Privacy statement 4Insurance

Stopzetten samenwerking met 4Insurance

Bij beëindiging van de samenwerking met de verwerkersverantwoordelijke (de 4Insurance relatie), zal de software inclusief alle data verwijderd worden van de 4Insurancesystemen -die worden gehost- voor de relatie. Daarvan leveren wij een proces-verbaal op, mede opgesteld door onze hostingprovider. ANVA is de leidende backoffice (applicatie/database) waarin alle financiële transacties vastliggen en daarmee deze dus wettelijk behouden blijft voor de verwerkersverantwoordelijke (de 4Insurance relatie). 4Insurance met onder andere AWI Connect de frontoffice-applicatie slechts volgt (wij lezen en schrijven in ANVA), wij na beëindiging dus niet gebonden zijn aan fiscale regels want de data is van de verwerkersverantwoordelijke.

Binnen de 4Insurance software zijn de volgende vormen van beëindigen denkbaar:

- Opzegging polis van de eindklant (zakelijk of particulier)
- Beëindiging aanstelling van een persoon/medewerker/agent
- Beëindiging contract tussen klant en 4Insurance

En gegevens van diverse gebruikers:

- Klant van 4Insurance, de Volmacht/Service Provider en haar agenten

Rechten van betrokkenen

Wil je inzage vragen in de gegevens die 4Insurance over je verwerkt en deze (laten) corrigeren, verwijderen of overdragen of de samenwerking stopzetten, dan is dit mogelijk door een verzoek op te sturen naar info@awisoftware.nl

Voor zover 4insurance de verantwoordelijke is van Uw persoonsgegevens, kan iedere betrokkene 4insurance verzoeken om zijn/haar persoonsgegevens te wijzigen, te verbeteren, aan te vullen, te verwijderen of af te schermen.

De verantwoordelijke geeft betrokkene binnen uiterlijk 4 weken antwoord. Wanneer de verantwoordelijke geen gevolg geeft aan het verzoek van de betrokkene, geeft hij uitleg over waarom het verzoek zonder gevolg is gebleven.

Privacy statement 4Insurance

Bijlage:

Bron: https://www.computable.nl/artikel/opinie/infrastructuur/6497942/1509029/post-gdpr-3-maatregelen-om-dataverkeer-binnen-je-netwerk-te-beveiligen.html?utm_source=computable.nl&utm_medium=email&utm_campaign=dagelijkse_update&utm_content=topartikelen

Ook netwerkoperators hebben met de eisen te maken doordat data op elke locatie en op elk punt tijdens de overdracht van en naar het datacenter moet worden beveiligd. Hoe weet u of uw netwerk veilig is? De onderstaande checklist voor gegevensbescherming kan helpen bij uw netwerkbeveiligingsstrategie.

Data in opslag wordt meestal beschermd door vier muren en idealiter ook met uitgebreide beveiligingsprotocollen en speciale hardware- en softwareoplossingen. Data is tijdens de overdracht echter relatief eenvoudiger te bemachtigen. Met simpele apparatuur kunnen cybercriminelen glasvezelkabels aftappen om toegang te krijgen tot informatie die binnen of tussen netwerken wordt overgedragen. Organisaties zouden daarom een gelaagde beveiligde beveiligingsaanpak moeten toepassen om al het dataverkeer van verbonden apparaten binnen het netwerk en van en naar het datacenter te beschermen.

1. **Veilige gegevensoverdracht via het netwerk**

End-to-end encryptie van het dataverkeer maakt de overgedragen informatie nutteloos voor hackers die gebruikmaken van aftap-apparatuur op de transport laag van netwerken. Maar er zijn nog meer encryptieoplossingen die het overwegen waard zijn. Als u ultra lage latency nodig heeft, zou u kunnen kiezen voor encryptie-oplossingen voor het dataverkeer op layer 1. Deze oplossingen beveiligen het dataverkeer met behoud van optimale doorvoersnelheden en minimalisatie van de latency. Het gebruik van protocolonafhankelijke technologie zorgt voor extra efficiëntie door de mogelijkheid om verschillende protocollen te versleutelen op dezelfde golflengte binnen de glasvezel. Het is raadzaam om gebruik te maken van encryptie bij de eindklant. Op deze manier kan de operator de netwerkdienst integraal beheren, terwijl de klant het beheer van de encryptiesleutels voor zijn rekening neemt. Als er minder hoge eisen aan de bandbreedte en latency worden gesteld, is het mogelijk om voor een minder belastende effectieve gegevensbescherming te zorgen met encryptie door een softwarematige virtual network function (VNF).

2. **Waarborg onder alle omstandigheden de beschikbaarheid van een veilig netwerk**

Als gevolg van GDPR moet data altijd opvraagbaar zijn, wat er ook gebeurt. Dat betekent dat u zeker moet zijn van de continuïteit van gegevensoverdracht en beschikbaarheid van het netwerk, zelfs als u te maken krijgt met een cyberaanval of een natuurramp. Het netwerk zou moeten voorzien in volledig redundante infrastructuurcomponenten (voeding, processors, switches enzovoort) en alternatieve netwerktrajecten die het mogelijk maken om het dataverkeer om te leiden en, waar nodig, te herstellen.

3. **Wees zeker van uw netwerkproviders en leveranciers**

Misschien voldoet uw netwerk wel aan de GDPR-eisen, maar doen uw leveranciers dat ook? Om optimale netwerkintegriteit te waarborgen moeten organisaties er zeker van zijn dat hun providers en leveranciers van netwerktechnologie veilige en goed gedocumenteerde procedures hanteren voor alle activiteiten, van de inkoop en fabricage van componenten, tot het ontwerp, de implementatie en het opereren van het netwerk.
Naarmate de reikwijdte van het netwerk groeit en de beveiliging complexer wordt, zullen ‘controllers’ en ‘verwerkers’ van data steeds vaker advies nodig hebben om GDPR-compliance en effectieve beveiliging van persoonsgegevens te waarborgen. Alleen door de handen ineen te slaan kunnen bedrijven en netwerkoperators er zeker van zijn dat data veilig is, waar het zich ook bevindt of beweegt.