Beveiligingsmaatregelen Archie CRM hostingomgeving

Archie Europe hanteert een autorisatiebeleid voor de Archie CRM hostingomgeving om te zorgen dat medewerkers alleen toegang hebben tot de informatie die strikt noodzakelijk is om hun werkzaamheden te verrichten.

Doelstelling autorisatiebeleid

Het autorisatiebeleid schept het kader voor de toegang en het gebruik van gegevens, applicaties en technische infrastructuur door middel van een pakket aan normen en eisen en de hieraan gerelateerde maatregelen.
Doelstelling van het autorisatiebeleid is het waarborgen van een gecontroleerde toegang tot, en gebruik van gegevens, applicaties en technische infrastructuur met betrekking tot de Archie CRM hostingomgeving.

Toegangsrechten worden geregistreerd. Registratie van service accounts en andere beveiligingscredentials anders dan de persoonlijke logins geschiedt in een beveiligde database. Alleen specifieke medewerkers hebben toegang tot de beveiligde database, kluizen (via Fingerprint), sleutels etc. waar zich informatie bevindt die toegang kan geven tot de cloudservers en/of data van klanten. Alleen een specifieke medewerker is (al dan niet in opdracht van de security/privacy officer) bevoegd om een gebuikersidentificatie af te geven/aan te maken.

De organisatie van informatiebeveiliging en communicatieprocessen binnen Archie Europe bv

Archie Europe bv beschikt over een actief informatiebeveiligingsbeleid. Archie Europe bv beschikt daarnaast over een security/privacy officer die beveiligingsbewustzijn stimuleert, de correcte omgang met persoonsgegevens controleert en maatregelen treft die toezien op naleving van het informatiebeveiligingsbeleid.

Medewerkers

Medewerkers van Archie Europe bv hebben een geheimhoudingsverklaring ondertekend. Er is daarnaast een “Ethische Code” binnen de organisatie welke ook door alle medewerkers ondertekend is. Medewerkers hebben op grond van de autorisatiesystematiek geen toegang tot meer data dan strikt noodzakelijk is voor hun functie.
Toegang tot data, die onder de verantwoordelijkheid van Archie Europe bv vallen, wordt alleen en slechts alleen door de eigenaar van de data verleend op persoonlijke titel. Dit geldt ook voor derden en medewerkers van het Archie hosting team.

Fysieke beveiliging en continuïteit van de middelen

Persoonsgegevens worden uitsluitend verwerkt in een omgeving (Archie CRM hostingomgeving) met bescherming tegen bedreigingen van buitenaf op apparatuur en locatie waarbij maatregelen zijn genomen om deze fysiek te beveiligen en de continuïteit van de dienstverlening te verzekeren.
De Archie CRM hosting is geïnstalleerd in een colocatie bij NorthC Datacenters. De beveiliging van de Archie hosting geschiedt door het internetverkeer middels een firewall te reguleren. Fysieke beveiliging van de hardware wordt afgehandeld door NorthC Datacenters.
NorthC Datacenters is ISO 27001, 9001, 14001 en ISAE 3402 Type 2 gecertificeerd. Daarnaast hebben zij een PCI DSS, NEN7501 en AM-IX certificaat. Fysieke toegang bij NorthC Datacenters is alleen mogelijk na aanmelding door de specifieke medewerkers van Archie Europe bv, waarbij het tonen van een geldig ID en biometrische controle van desbetreffende medewerker noodzakelijk is. Dit geldt ook voor eventueel ingehuurde derden. De racks zijn ook beveiligd door cijfersloten. De code van deze sloten is alleen bekend bij specifiek aangewezen medewerkers.
Er worden periodiek versleutelde back-ups gemaakt van de data in de Archie hostingomgeving ten behoeve van de continuïteit van de dienstverlening welke vertrouwelijk worden behandeld en bewaard in een zowel fysiek als virtueel beveiligde omgeving. Deze worden fysiek op een andere locatie bewaard. Daarnaast is er een beveiligde failover omgeving beschikbaar op een derde locatie.

Beveiliging Archie

De inzet van de AMEE laag (Archie Multi-Tier Environment Engine – tussenlaag software) beschermt de Archie database op de SQL server doordat Archie gebruikers via de client nooit rechtstreeks verbinding maken met de SQL server. De communicatie met de database wordt afgehandeld via geregistreerde SQL gebruiker (username en password zoals geregistreerd binnen de SQL server omgeving). Het Client-Server verkeer is versleuteld volgens de AES standaard. Het web verkeer is versleuteld middels een SSL certificaat.

Netwerk- en serverbeveiliging en -onderhoud

De netwerkomgeving waarbinnen data wordt verwerkt is strikt beveiligd. Op wachtwoorden worden cryptografische maatregelen toegepast en verkeersstromen worden gescheiden.
Daarnaast zijn er maatregelen geïmplementeerd tegen misbruik en aanvallen.
De beveiliging van de omgeving waarbinnen persoonsgegevens in de hostingomgeving van Archie worden verwerkt wordt gemonitord.
Op de systemen worden periodiek de laatste (beveiliging)patches geïnstalleerd op basis van patchmanagement.
Er wordt jaarlijks een Pen- en Hacktest uitgevoerd door een gespecialiseerd bureau zodat de meest actuele beveiligingsverbeteringen kunnen worden geïmplementeerd.