altijd tijd.

voor de kleine lettertjes

aiono.ai

Jouw ai-klantenservice

grote plannen, kleine letters.

Dit beleid beschrijft hoe Aiono persoonsgegevens, audio-opnames en bedrijfsinformatie beschermt tegen ongeoorloofde toegang, verlies of misbruik. Het geldt voor alle medewerkers, systemen en diensten van Aiono.

Informatiebeveiligingsbeleid Aiono / Bepromptly B.V.

Beveiligingsprincipes

• Vertrouwelijkheid: Toegang tot gegevens is beperkt tot bevoegde personen op basis van rol en noodzaak.
• Integriteit: Gegevens worden beschermd tegen ongewenste wijziging door logging, versiebeheer en toegangscontrole.
• Beschikbaarheid: Diensten worden redundant gehost in beveiligde datacenters met monitoring en automatische failover.

Technische maatregelen

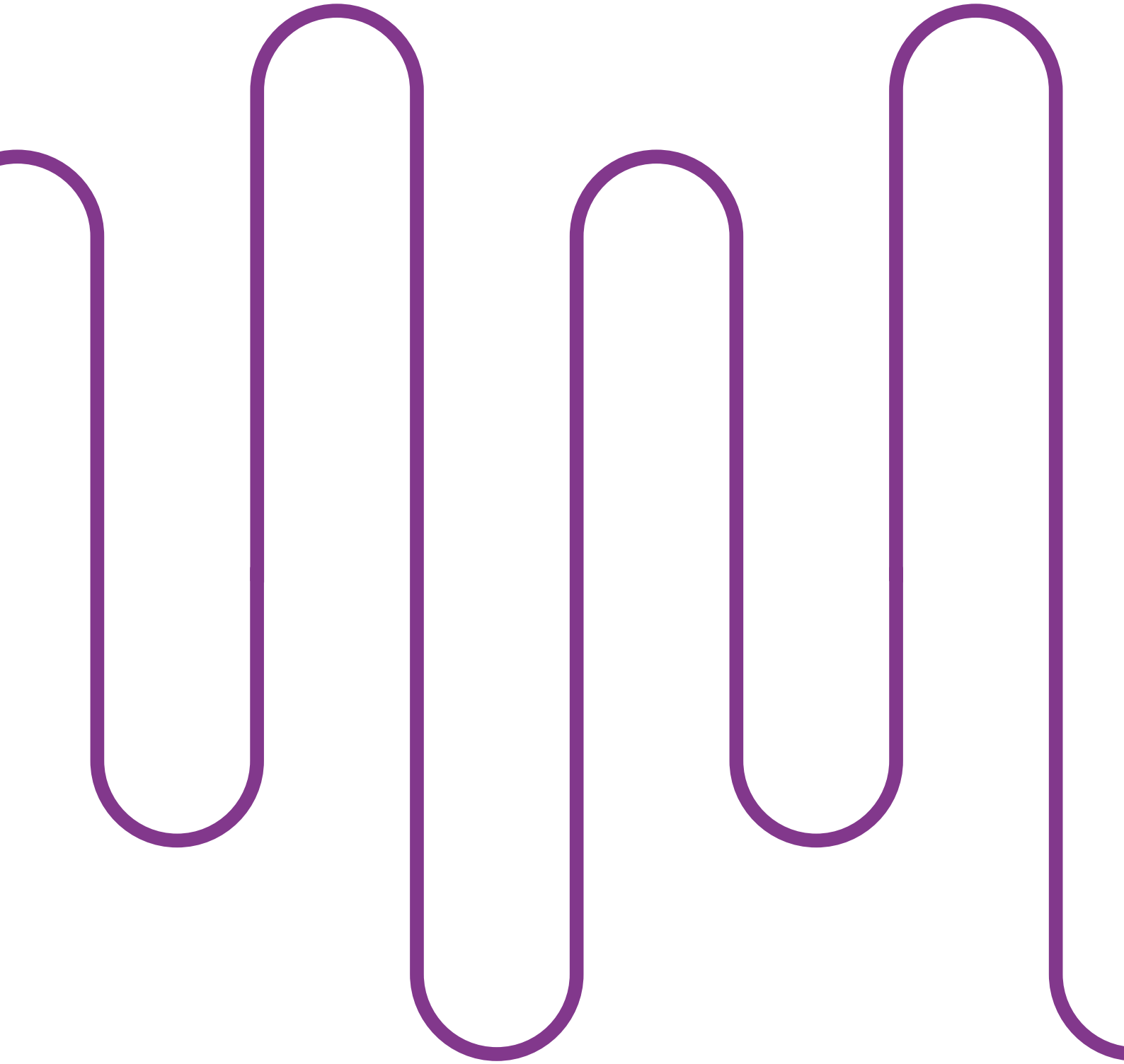
• Encryptie van data in opslag (AES-256) en tijdens verzending (TLS 1.2+).
• Sterke authenticatie (2FA) voor alle beheerders- en klantportalen.
• Netwerkbeveiliging via firewalls, DDoS-bescherming en intrusion detection.
• Gescheiden productie-, test- en ontwikkelomgevingen.
• Regelmatige beveiligingsupdates en kwetsbaarheidsscans.

Organisatorische maatregelen

• Medewerkers hebben een geheimhoudingsplicht (NDA) en volgen jaarlijks security- en privacytraining.
• Toegangsrechten worden periodiek beoordeeld en ingetrokken bij vertrek.
• Incident- en datalekprocedure conform AVG, inclusief melding aan de Functionaris Gegevensbescherming (FG).
• Contractuele verplichtingen en audits bij subverwerkers (zoals hostingpartners).

Continuïteit en toezicht

• Back-ups worden dagelijks gemaakt, versleuteld opgeslagen en periodiek getest op herstel.
• Jaarlijkse interne audit en herziening van dit beleid.
• Beveiligingsincidenten worden geregistreerd, geëvalueerd en gebruikt ter verbetering van processen.



aiono.ai