

clubwize
grip op je vereniging

VEILIGHEID EN GEGEVENSVERWERKING

Veiligheid is geen bijzaak

Je vertrouwt ons de gegevens toe van je leden, vrijwilligers en teams. Hier lees je waar die gegevens staan, hoe we ze beschermen en hoe we de software controleren.

Database en bestanden staan in de EU

De software, de database en je bestanden staan op servers in de EU. Voor enkele diensten, zoals e-mail versturen, werken we met partijen buiten de EU. Wie dat zijn en welke afspraken er gelden, staat in de verwerkersovereenkomst.

HOE WE JE GEGEVENS BESCHERMEN

- ✓ **Elke organisatie apart**
  Elke organisatie heeft een eigen, afgeschermd deel van de database.
- ✓ **Gevoelige sleutels versleuteld**
  De sleutels voor koppelingen met andere systemen slaan we versleuteld op.
- ✓ **Raden wordt tegengehouden**
  Herhaalde inlogpogingen blokkeren we tijdelijk. Dat beschermt tegen het raden van wachtwoorden.
- ✓ **Wijzigingen vastgelegd**
  Wijzigingen in persoonsgegevens leggen we vast: wie wat wanneer heeft gewijzigd.
- ✓ **Altijd een versleutelde verbinding**
  De verbinding met de software is altijd versleuteld (https).
- ✓ **Wachtwoorden onleesbaar**
  We slaan wachtwoorden niet leesbaar op, alleen als onomkeerbare code (een hash).
- ✓ **Inloggen in twee stappen**
  Beheerders kunnen naast hun wachtwoord een code gebruiken uit een app op hun telefoon.
- ✓ **Automatische back-ups**
  De database wordt beheerd door onze hostingpartij en heeft automatische back-ups.

Hoe we de software zelf controleren, lees je op de achterkant.

CONTROLE EN VERANTWOORDING

Zo controleren we de software

Elke nacht op bekende lekken

Onze software gebruikt externe onderdelen. Die controleren we elke nacht automatisch op bekende kwetsbaarheden, aan de hand van openbare registers zoals de CVE-lijst.

Eigen code en servers gescand

Onze eigen broncode scannen we automatisch op bekende typen beveiligingsfouten. De systeemsoftware van onze servers controleren we op ernstige kwetsbaarheden.

Alarm bij een nieuwe bevinding

Vindt een controle iets nieuws, dan gaat er een alarm af. Lossen we een bevinding bewust niet op, dan leggen we de reden vast.

Elke week updates klaar

Dependabot, een dienst van GitHub, zet elke week updates van die externe onderdelen klaar, voor de software en voor de apps.

AI zoekt mee naar zwakke plekken

Bij risicovolle wijzigingen en tijdens beveiligingsaudits laten we de broncode ook door AI controleren, gericht op kwetsbaarheden. Die controle kijkt alleen naar de code, nooit naar de gegevens van je organisatie. Wat de AI vindt, beoordelen we zelf.

AI-regels vastgelegd

Voor onze eigen AI-functies hebben we vastgelegd welke regels uit de Europese AI-verordening gelden en in welke risicocategorie ze vallen.

Datalek binnen 48 uur gemeld

In de verwerkersovereenkomst staat dat we een datalek binnen 48 uur na ontdekking aan je melden.

Lek gevonden? Meld het ons

Meldingen van beveiligingslekken behandelen we volgens de leidraad van het Nationaal Cyber Security Centrum (NCSC).

Twintig jaar ervaring

Achter elke controle staat meer dan twintig jaar ervaring met software voor de overheid en het bedrijfsleven.

Lees het zelf na

Alles staat openbaar op onze website. Inloggen is niet nodig.

clubwize.nl/veiligheid Hoe we gegevens beschermen en de software controleren.

clubwize.nl/kwetsbaarheid-melden Een beveiligingslek aan ons melden.

clubwize.nl/verwerkersovereenkomst De volledige verwerkersovereenkomst.

clubwize
grip op je vereniging

Scan voor de veiligheidspagina

www.clubwize.nl

support@clubwize.nl