
VEILIGHEIDSMATREGELEN NNOTE 2025

1. | ENCRYPTIE

Alle data binnen Nnote is versleuteld met de AES-256-methode. Dit betekent dat alle gegevens worden beveiligd met een encryptiesleutel van 256 bits, een van de veiligste versleutelingstechnieken die wereldwijd wordt toegepast.

2. | ALGEMENE BEVEILIGINGSCHECKLIST

SSL-certificaat – Alle communicatie verloopt via een beveiligde verbinding.

DDoS-bescherming – Het platform is beschermd tegen DDoS-aanvallen.

Beveiligde serverruimte – Servers bevinden zich in een fysiek beveiligde ruimte met cameratoezicht en toegangscontrole.

Serverlocatie Nederland – Nnote draait op servers die gevestigd zijn in Nederland (Amsterdam).

Back-ups – Data wordt opgeslagen op twee gescheiden locaties om continuïteit te garanderen.

Tweestapsverificatie (2FA) – Nnote biedt 2FA als extra beveiligingslaag bij het inloggen om ongeautoriseerde toegang te voorkomen.

Beveiligde werkplekken – Apparatuur waarop Nnote wordt ontwikkeld en beheerd, bevindt zich in gecontroleerde en beveiligde omgevingen.

Up-to-date software – Het systeem draait altijd op recente versies van gebruikte software.

Continue monitoring en tests – Dagelijkse tests en continue monitoring van errorlogs.

3. | STRIKTE SLA MET ONTWIKKELAARS

Nnote hanteert strikte serviceafspraken (SLA) met haar ontwikkelaars. Dit betekent dat bij kritieke problemen – zoals niet-functionerende onderdelen – snel actie wordt ondernomen. In dergelijke gevallen heeft Nnote recht op een snelle oplossing binnen de kortst mogelijke tijd.

4. | BEVEILIGINGS- EN GEGEVENSBESCHERMINGSAFSPRAKEN

Nnote en haar ontwikkelaars hanteren strikte afspraken rondom gegevensbescherming en privacy. Dit houdt in:

- **Geen toegang tot gevoelige data** – Zowel Nnote als de ontwikkelaars hebben géén inzicht in gegevens van melders, meldingen, chats, vertrouwenspersonen of andere vertrouwelijke informatie binnen het systeem.
- **Geen toegang tot automatisch gegenereerde rapportages of bedrijfsdata** – Alle vertrouwelijke gegevens blijven volledig afgeschermd.

5. | INZICHTELIJKE GEGEVENS

Om het platform goed te laten functioneren en abonnementen te beheren, hebben zowel Nnote als de ontwikkelaars enkel toegang tot:

- Bedrijfsnamen die aan het systeem zijn toegevoegd
- Namen van externe vertrouwenspersonen
- Systeeminstellingen, zoals de voorkeurtaal van organisaties

Deze informatie wordt uitsluitend gebruikt voor het beheren van abonnementen en het snel opsporen van eventuele technische fouten binnen een organisatie. Deze gegevens worden in geen geval ongevraagd gedeeld met derden.