GROENEWEGEN&LUKAART
bedrijven (ver)kopen, waarderen en financieren

# BEVEILIGING

## Introductie

De doelstelling voor Groenewegen & Lukaart is het zo veilig mogelijk leveren van onze diensten, het beschermen van klantgegevens en het bewaken van het vertrouwen van onze klanten. Onze visie is vastgelegd in het Informatiebeveiligingsbeleid. Dit beleid omvat meerdere beveiligingsmaatregelen om gegevens te beschermen tegen lekken, verlies en diefstal. Daarmee handhaven we de integriteit, vertrouwelijkheid en beschikbaarheid van de gegevens van onze klanten.

## Information Security Officer

Voor al uw vragen of meldingen over onze beveiliging kunt u terecht bij de Information Security Officer van Groenewegen & Lukaart, namelijk:

| | |
|---|---|
| Naam: | T.W.J.H.H. (Tamara) Putmans |
| Tel: | 010 522 68 00 |
| E-mail: | security@groenewegen&lukaart.nl |

## Leveranciers

Ook met leveranciers en sub-verwerkers hebben we afspraken gemaakt over de beveiliging en continuïteit van de dienstverlening, in lijn met het informatiebeveiligingsbeleid van Groenewegen & Lukaart. Wij streven ernaar om met alle sub-verwerkers een verwerkersovereenkomst conform de AVG wetgeving af te sluiten.
Specifiek beoordelen wij onze leveranciers op aanwezigheid van certificeringen zoals ISO 27001 en/of ISAE 3402. ISO 27001 is een internationale norm gepubliceerd door de Internationale Standaardisatie Organisatie (ISO) en beschrijft hoe informatiebeveiliging in een bedrijf kan worden beheerst. ISAE 3402 betreft een audit standaard over uitbestede processen. Wanneer leveranciers over een ISAE 3402 Type II rapportage beschikken beoordelen wij die periodiek om vast te stellen dat de interne beheersingsmaatregelen effectief werken.

## Gecertificeerde Hosting

Groenewegen & Lukaart maakt gebruik van cloud hosting in plaats van on-premise hosting. Beveiligingsverantwoordelijkheden worden gedeeld door Groenewegen & Lukaart en de serviceprovider. Wij maken uitsluitend gebruik van ISO 27001

gecertificeerde datacenters binnen Nederland.

## Data versleuteling

We gebruiken cryptografische maatregelen (encryptie of versleuteling) om de vertrouwelijkheid van gevoelige en geheime informatie te beschermen en om de authenticiteit van gebruikers te kunnen vaststellen. Voor het elektronisch transport maakt Groenewegen & Lukaart altijd gebruik van toonaangevende versleutelingstechnologieën als HTTPS en Transport Layer Security (TLS).

## E-mail

Alle e-mail die Groenewegen & Lukaart verstuurd en ontvangt wordt verwerkt door mailservers in uitsluitend gecertificeerde datacenters. Tevens maken wij voor het verzenden van bijlagen gebruik van AttachingIT waarmee bijlagen veilig gedeeld kunnen worden.

## Security Awareness

Met medewerkers van Groenewegen & Lukaart (zowel intern als extern) worden geheimhoudingsverklaringen overeengekomen en informatiebeveiligingsafspraken gemaakt. Ook stimuleren wij het bewustzijn, opleiding en training ten aanzien van privacy en informatiebeveiliging.

## Meldplicht datalekken

De meldplicht datalekken in de AVG eist dat eventuele datalekken naar aanleiding van een beveiligingsincident gemeld worden aan de toezichthouder. De “Beleidsregels meldplicht datalekken” van de Nederlandse Autoriteit Persoonsgegevens geven hierover nadere informatie. Wij zullen u tijdig, juist en volledig informeren over relevante incidenten, zodat u aan de wettelijke vereisten kunt voldoen.

## Responsible Disclosure

Groenewegen & Lukaart wil zich inspannen voor optimale veiligheid en hecht grote waarde aan de security van haar systemen. Toch valt nooit uit te sluiten dat er zwakke plekken voorkomen. Als u een zwakke plek heeft gevonden in www.veermanlukaart.nl, horen we dat graag van u. We zullen dan zo snel mogelijk maatregelen nemen. Groenewegen & Lukaart verzoekt bij vermeende kwetsbaarheden altijd gebruik te maken van bovenstaand e-mailadres. Meldingen of openbaar maken van informatie via sociale media wordt ten stelligste afgeraden om mogelijke risico’s voor betrokkenen zo beperkt mogelijk te houden.

*Rapporteer wel:*

- Persistent Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF/XSRF)
- Niet werkende authenticatie
- Het kunnen omzeilen van ingestelde privacy / rechten
- Remote Code Execution

*Rapporteer geen*:
• Username dictionairy attack
• Self-XSS
• Missende / niet streng geconfigureerde DNS SPF records
• Social hacking
• Publiek toegankelijke login pagina’s voor admin/cms omgevingen
• Veiligheidsproblemen in third-party apps die niet opgelost zijn in de laatste versie
• Denial of Service Vulnerabilities
• Missende HSTS header
• Missende DNSSEC
• Missende CSP header
• Aanvallen waarbij een DNS takeover nodig is