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

BEVEILIGING

Introductie

De doelstelling van Groenewegen & Lukaart Corporate Finance B.V. (hierna te noemen: 'Groenewegen & Lukaart') is het zo veilig mogelijk leveren van diensten, het beschermen van klantgegevens en het bewaken van het vertrouwen van klanten. De visie van Groenewegen & Lukaart is vastgelegd in haar informatiebeveiligingsbeleid dat is opgesteld volgens de internationale norm ISO27001. Dit beleid omvat meerdere beveiligingsmaatregelen om gegevens te beschermen tegen lekken, verlies en diefstal. Daarmee handhaaft Groenewegen & Lukaart de integriteit, vertrouwelijkheid en beschikbaarheid van de gegevens van klanten.

Leveranciers

Met leveranciers en sub-verwerkers heeft Groenewegen & Lukaart afspraken gemaakt over de beveiliging en continuïteit van de dienstverlening, in lijn met het informatiebeveiligingsbeleid. Groenewegen & Lukaart streeft ernaar om met alle sub-verwerkers een verwerkersovereenkomst conform de AVG-wetgeving af te sluiten.

Specifiek beoordeeld Groenewegen & Lukaart de leveranciers op aanwezigheid van certificeringen zoals ISO27001 en/of ISAE3402. Wanneer leveranciers over een ISAE3402 Type II rapportage beschikken, beoordeeld Groenewegen & Lukaart deze periodiek om vast te stellen dat de interne beheersmaatregelen 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. Groenewegen & Lukaart maakt uitsluitend gebruik van ISO27001 gecertificeerde datacenters binnen de Europese Unie.

Data versleuteling

Groenewegen & Lukaart gebruikt cryptografische maatregelen (encryptie) om de vertrouwelijkheid van gevoelige en geheime informatie te beschermen en om de authenticiteit van gebruikers vast te kunnen stellen. Voor het elektronisch transport maakt Groenewegen & Lukaart altijd gebruik van toonaangevende versleutelingstechnologieën zoals HTTPS en Transport Layer Security (TLS).

Fysieke beveiliging

Informatiebeveiliging gaat voor Groenewegen & Lukaart verder dan alleen de systemen en applicaties. Groenewegen & Lukaart hecht daarom ook veel waarde aan fysieke beveiliging van gebouwen, archiefruimtes, desktops, laptops en andere bedrijfsmiddelen waar informatie over klanten te vinden is. Om deze te beveiligen heeft Groenewegen & Lukaart verschillende maatregelen getroffen, namelijk een combinatie van organisatorische, bouwkundige en elektronische maatregelen.

E-mail

Alle e-mail die Groenewegen & Lukaart verstuurd en ontvangt wordt verwerkt door mailservers in uitsluitend gecertificeerde datacenters. Tevens maakt Groenewegen & Lukaart gebruik van een oplossing voor het veilig (encrypt) ontvangen, versturen en delen van bestanden.

Beveiligingsbewustzijn

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

Meldplicht datalekken

De meldplicht datalekken volgens de AVG-wetgeving 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. Groenewegen & Lukaart zal 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 beveiliging van haar systemen. Toch valt nooit uit te sluiten dat er zwakke plekken voorkomen. Als u een zwakke plek heeft gevonden op de website van Groenewegen & Lukaart, dan horen we dat graag van u. Er zullen dan zo spoedig mogelijk maatregelen worden genomen.

Information Security Officer (ISO)

Voor al uw vragen of meldingen over de beveiliging van Groenewegen & Lukaart kunt u terecht bij de Information Security Officer van Groenewegen & Lukaart door te bellen naar 010-5226800 of een e-mail te sturen aan security@groenewegen-lukaart.nl. Groenewegen & Lukaart verzoekt bij vermeende kwetsbaarheden altijd contact op te nemen. 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 disctionairy attack
- Self-XSS
- Missende / niet streng geconfigureerde DNS SPF records
- Social hacking
- Publiek toegankelijke login pagina's voor admin / cms omgevingen
- Veiligheidsproblemen in third-partij apps die niet opgelost zijn in de laatste versie
- Denial of Service Vulnerabilities