

**SpecsHEET ECOCHARTING SOFTWARE**  
**Juni 2024**



**Toelichting SpecsHEET**

In dit document lichten we kort toe welke functionaliteit deze maand wordt ontwikkeld in de software van Ecocharting. Omdat de CSRD een nieuw onderwerp is en we onze ontwikkeling aansturen op basis van feedback van klanten, duurzaamheidsexperts en accountants, pinnen we de software roadmap niet voor de lange termijn vast.

<b>RACE</b>	test, acceptatie, demo, productie
<b>Data Warehouse</b>	Data wordt opgeslagen in Europese data warehouse, namelijk in Frankfurt (DE).
<b>ISO-27001</b>	data warehouse via AWS is ISO gecertificeerd.
<b>Access-control</b>	Role-based access control zorgt ervoor dat toegang wordt toegewezen op basis van de rol van teamleden .
<b>Back-ups</b>	Iedere 24 uur maken we een backup van de database, daarnaast maken we altijd voor een nieuwe release een backup van het gehele systeem.
<b>Retentieperiode</b>	De retentieperiode van onze backups is altijd 7 dagen. Hierdoor kunnen we altijd tot 7 dagen terug in de tijd.
<b>Versleuteling</b>	Zowel tijdens versturen als in stilstand (in transit & at rest)
	Zowel via sha256 als Encryption SDK van AWS.
<b>Opschalen</b>	Kubernetes framework stelt ons in staat om zowel horizontaal als verticaal onze infrastructuur op te schalen.
<b>Servicedesk</b>	Uptime van het systeem van 99.5% per maand.
	Voor urgente support tickets hanteren wij een responstijd van 24 uur.
	Verdere details beschikbaar in SLA overeenkomst. Zie link onderaan pagina 2.
<b>AVG-compliance</b>	Dit is opgenomen in de dataverwerkersovereenkomst. Zie link onderaan pagina 2.
<b>Authenticatie</b>	We gebruiken Auth0 als identity-provider.
<b>SSO</b>	auth0 als identity provider (o.a. Google & Microsoft login)
<b>Integratie</b>	Het is mogelijk om van zelf gegenereerde resultaten binnen Ecocharting een export te maken. Denk hierbij aan de shortlist, materialiteitsmatrix en dergelijke.
	Ecocharting beschikt over een REST API. De gebruiker krijgt toegang via Auth0 en vraagt een tijdelijke bearer token aan. De wordt gebruikt om GET, POST en PUT calls uit te voeren.
	Monitoring i.c.m. rate limiting is actief op om misbruik van de API te voorkomen.



ECOCHARTING

## Ecocharting Beveiligingsverklaring

Ecocharting is een cloud-gebaseerde oplossing. We geven prioriteit aan de beveiliging van onze softwareoplossingen door middel van uitgebreide maatregelen die zijn ontworpen om data te beschermen en hoge normen van privacy en integriteit te handhaven. Onze cloudomgeving wordt gehost in Frankfurt, Duitsland, en maakt gebruik van de wereldwijd erkende infrastructuur van AWS, die **gecertificeerd** is volgens **ISO/IEC 27001:2022**, 27017:2015, 27018:2019, 27701:2019, 22301:2019, 20000-1:2018, 9001:2015 en CSA STAR CCM v4.0. Dit zorgt voor naleving van strenge beveiligings- en compliance-normen.

De gegevens binnen ons platform zijn zowel tijdens transport als in rust beveiligd door middel van **versleuteling** met het AES-256-protocol, samen met geavanceerde algoritmes uit het AWS Encryption SDK. Dit garandeert een hoog niveau van gegevensvertrouwelijkheid en integriteit. Onze toewijding aan gegevensbeveiliging wordt verder bevestigd door de **'A'-beoordeling** die onze cloudomgeving kreeg bij **SSL LABS Server-tests**.

Wat betreft **gegevensopslag en -bewaring** zorgen we ervoor dat gegevens met betrekking tot CSRD-rapportage veilig worden opgeslagen totdat de gebruiker aangeeft dat ze moeten worden verwijderd. Dit beleid ondersteunt toekomstige auditprocessen door accountants en verhoogt de betrouwbaarheid en traceerbaarheid van rapportage. Alle gegevenswijzigingen binnen de Ecocharting-omgeving worden nauwkeurig gelogd, zodat elke wijziging kan worden getraceerd om verantwoordelijkheid en forensische analyse mogelijk te maken. Deze logs worden bewaard in overeenstemming met boekhoudkundige en bewijseisen, totdat ze niet langer nodig zijn of op verzoek van de gebruiker.

Onze **back-up strategie** omvat dagelijkse snapshots met een retentiebeleid van een week, wat betekent dat we snel kunnen herstellen van incidenten met minimaal gegevensverlies en een maximale uitvaltijd van 24 uur, wat onze robuuste Recovery Point Objectives en Recovery Time Objectives weerspiegelt.

Toegang tot de Ecocharting-software is mogelijk via een externe identity provider (IdP). Als IdP gebruiken wij Auth0. Hierdoor is het tevens mogelijk om via Single-Sign-On (SSO) toegang te krijgen tot de Ecocharting applicatie. Het is dus mogelijk je Google account of Microsoft Azure AD account te gebruiken om toegang te krijgen tot Ecocharting. Dit helpt voor een nog meer verbeterde beveiliging en efficiëntie. Daarnaast communiceert onze cloudoplossing veilig met externe systemen zoals Sendgrid, beveiligd via veilige **API-gateways** om cyberbedreigingen tegen te gaan.

Momenteel beschikt Ecocharting over een **REST API** voor intern gebruik, uiteindelijk zal deze beschikbaar worden gemaakt voor de gebruikers van Ecocharting. De API biedt een robuuste en flexibele oplossing voor data-integratie binnen de Ecocharting-applicatie. Het is ontworpen als een REST API, compatibel met diverse systemen en programmeertalen via standaard **HTTP-methoden** zoals GET, POST, PUT en DELETE, wat eenvoudige gegevensbeheer en -uitwisseling mogelijk maakt. De API ondersteunt schaalbaarheid en beveiliging, maakt gebruik van Auth0 voor authenticatie en ondersteunt OAuth 2.0 en OpenID Connect (OIDC). Gebruikers zullen API-sleutels kunnen aanmaken en beheren via een beheerinterface, met eventueel Machine-To-Machine (M2M) API-tokens beschikbaar voor verbeterde autorisatie.

Lees tot slot onze *end-user license agreement* en *data processing agreement* om precies te begrijpen hoe en waarom we gegevens verwerken. U kunt deze documenten bekijken door de volgende URL te bezoeken: <https://ecocharting.com/terms-agreement/>