# BEVEILIGINGSRAPPORT

In dit rapport worden de beveiligingsmaatregelen van onze websites www.theonlinescientist.com, www.liesbethsmit.com en www.stephanvanduin.com en onze bedrijven besproken volgens de Algemene Verordening Gegevensbescherming.

*25 mei 2018*

## DATAVERZAMELING

Wij verzamelen/verwerken alleen gegevens die noodzakelijk zijn voor de uitvoering van een opdracht en algemene werkzaamheden. Bijvoorbeeld de emailadressen van klanten die een e-boek op onze website bestellen zodat we het e-boek op kunnen sturen.  Of wanneer het noodzakelijk is om te voldoen aan een wettelijke verplichting, of het versturen van facturen, offertes en het organiseren van hosting en domeinnamen.

Wij verzamelen mogelijk de volgende gegevens van onze klanten en bezoekers van onze website. Klanten zijn de partijen die ons hebben ingehuurd om voor ze te werken of waarmee we potentieel een klantrelatie aangaan.

- Voornaam
- Achternaam
- Emailadres
- Adres
- Telefoonnummer
- Rekeningnummer
- Website logingegevens: gebruikersnaam, email en wachtwoord
- (KVK nummer)

Deze gegevens worden als volgt verwerkt:

Ze worden lokaal op onze computers opgeslagen in Word, Excel of PDF, of via email (Gmail, Google Suite) naar ons verstuurd. Kunnen worden opgeslagen als backup bij DropBox (US) of Google Drive, en verwerkt in onze factuur software (Informer, NL) of bij onze bank (ING, KNAB) worden opgeslagen. Backups van alle bestanden worden op een externe harde schijf bewaard (WD Passport).

## BEVEILIGINGSMAATREGELEN VOOR HET VERWERKEN VAN GEGEVENS

Onze computers zijn encrypted en beschermd met een sterk wachtwoord. Updates worden direct uitgevoerd en computers zijn beschermd met een firewall en anti-virus software van Bitdefender. Backups worden in realtime uitgevoerd naar de cloud (DropBox) en dagelijks naar een externe harde schijf.

Onze email is beschermd met sterke wachtwoorden, en 2-factor authenticatie.

Met Google, DropBox hebben wij een verwerkersovereenkomst en zij verwerken deze gegevens volgens de Privacy Shield. Deze websites zijn beveiligd met SSL.

Wij verwerken eventuele extra informatie die de klant ons geeft uitsluitend voor het uitvoeren van de opdracht en niet voor andere doeleinden. Wij delen deze informatie niet met derde partijen tenzij dit onderdeel uitmaakt van de overeenkomst.

## BEVEILIGING VAN ONZE WEBSITE

De enige persoonsgegevens die wordt verzameld via de website zijn de logingegevens van de beheerders van de website: Naam en Emailadres.

De website liesbethsmit.com is beveiligd met een Let’s Encrypt SSL certificaat, en elke pagina wordt geforceerd om via SSL (HTTPS) getoond te worden.

Updates worden dagelijks uitgevoerd. Backups worden opgeslagen via ManageWP op Amazon S3 server in Europa, met HTTPS toegang, two-factor authentication, en monitoring

van de veiligheid. Er worden dagelijks backups gemaakt die ook op Dropbox worden opgeslagen.

Het data-center in Amsterdam waar de server van de website staat, heeft ISO 27001certification.

De website wordt dagelijks via ManageWP gecontroleerd op malware, vulnerabilities, en web trust van Google Safe Browsing, Norton Safe Web, PhishTank, SiteAdvisor, Sucuri Malware Labs, SpamHaus DBL, Yandex (via Sophos), en ESET. Backups worden dagelijks gemaakt.

Gegevens die via het contactformulier worden verzonden worden encrypted verstuurd naar ons emailadres en niet lokaal in een database opgeslagen.

De website data wordt opgeslagen in een met sterk wachtwoord beveiligde MySQOL database.

WordPress specifieke beveiliging:

- Alle gebruikers hebben 2-factor authentication
- Beveiliging via SSL
- Toegang tot de .htaccess en wp-config.php files is afgeschermd.
- XML-RPC is uitgeschakeld
- Bad bots worden geblokkeerd
- DDOS aanvallen worden gemitigeerd
- SQL Injection Attacks, Cross Site Scripting (XSS) worden tegen gegaan
- Logins van beheerders worden gemonitord zodat er geen toegang is door ongeauthoriseerde gebruikers.
- IP adressen worden na 3 verkeerde logins op een blacklist gezet en voor 30 minuten geweerd.
- Toegang tot PHP files van de website is geblokkeerd.
- Gebruikers die met admin gebruikersnaam willen inloggen worden verbannen van de site.

- Veranderingen in files op de website worden gemonitord en emails worden verstuurd wanneer er files worden aangepast.
- Gebruikers die in korte tijd veel 404 errors veroorzaken (10 binnen 5 minuten), wat een mogelijk veiligheidsrisico is, worden permanent van de website verbannen.
- Beheerders van de site moeten een sterk wachtwoord hebben.
- Er wordt twee keer per dag gescand op malware, blacklisting status, website errors, en verlopen software.
- WordPress, Plugin en Thema Updates worden automatisch geinstalleerd. Wanneer er verouderde software op de site wordt gebruikt dan wordt er een extra beveiligingslaag aangezet.
- Er wordt twee keer per dag gechecked voor updates van de software en plugins.

## OPVRAGEN, WIJZIGEN, VERWIJDEREN VAN DATA

Bij een verzoek voor het opvragen en verwijderen van persoonsgegevens kunnen wij dit alleen doen wanneer het geen conflict oplevert met het moeten bewaren van financiële data voor 7 jaar volgens onze administratie.

Verstuur een email naar info@liesbethsmit.com en wij kunnen alle informatie versturen, wijzigen, of verwijderen.