x

Verwerkersovereenkomst FOLEON

20 mei 2019

Artikel 1: Toepasselijkheid

1.1 Door het gebruik van de diensten van FOLEON uit hoofde van de licentieovereenkomst (de "Licentieovereenkomst"), zoals door het opmaken en publiceren van Publicaties en/of gebruikmaking van Formulieren, kan sprake zijn van het verwerken van persoonsgegevens in de zin van artikel 4.2 Algemene Verordening Gegevensbescherming ("AVG"). Voor zover u door gebruikmaking van de diensten uit hoofde van de Licentieovereenkomst persoonsgegevens verwerkt en deze verwerking valt onder de reikwijdte van de AVG, is het bepaalde in de onderhavige verwerkersovereenkomst (de "Overeenkomst") van toepassing.

Artikel 2: Onderwerp en doeleinden

2.1 FOLEON (de "Verwerker") verbindt zich onder de voorwaarden van deze Overeenkomst, om in uw opdracht persoonsgegevens te verwerken. U wordt hierna aangeduid als de "Verwerkingsverantwoordelijke".

2.2 De Verwerker heeft gezien de aard van de dienstverlening uit hoofde van de Licentieovereenkomst geen inzicht in de aard van en de soort van persoonsgegevens die door Verwerker in het kader van de werkzaamheden als bedoeld in het vorige lid worden verwerkt en de categorieën van de betrokkenen van wie deze afkomstig zijn. Verwerkingsverantwoordelijke geeft opdracht tot verwerking van alle categorieën van persoonsgegevens en betrokkenen, voor zover deze door Verwerkingsverantwoordelijke middels de diensten van Verwerker worden verwerkt.

2.3 De verwerking van persoonsgegevens door Verwerker zal slechts plaatsvinden in het kader van het opslaan door Verwerker op de servers van Verwerker of door Verwerker ingeschakelde derden, van de door of namens Verwerkingsverantwoordelijke gemaakte online publicaties en/of formulieren. Verwerker zal de persoonsgegevens niet voor enig ander doel verwerken dan zoals door Verwerkingsverantwoordelijke is vastgesteld. Verwerkingsverantwoordelijke zal Verwerker op de hoogte stellen van de verwerkingsdoeleinden voor zover deze niet reeds in deze Overeenkomst zijn genoemd.

2.4 De in opdracht van Verwerkingsverantwoordelijke te verwerken persoonsgegevens blijven eigendom van Verwerkingsverantwoordelijke en/of de betreffende betrokkenen.

Artikel 3: Verplichtingen algemeen

3.1 Verwerker is slechts verantwoordelijk voor de verwerking van de persoonsgegevens onder deze Overeenkomst, overeenkomstig de instructies van Verwerkingsverantwoordelijke en onder de uitdrukkelijke (eind-) verantwoordelijkheid van Verwerkingsverantwoordelijke. Voor de overige verwerkingen van persoonsgegevens, waaronder in ieder geval begrepen, maar niet beperkt tot, de verzameling van de persoonsgegevens door de Verwerkingsverantwoordelijke, verwerkingen voor doeleinden die niet door Verwerkingsverantwoordelijke aan Verwerker zijn gemeld, verwerkingen door derden en/of voor andere doeleinden, is Verwerker in geen geval verantwoordelijk.

3.2 Verwerkingsverantwoordelijke garandeert dat de inhoud, het gebruik en de opdracht tot de verwerkingen van de persoonsgegevens zoals bedoeld in deze Overeenkomst niet onrechtmatig zijn en geen inbreuk maken op enig recht van derden waaronder de betrokkenen. Verwerkingsverantwoordelijke vrijwaart Verwerker voor aanspraken van derden, autoriteiten daaronder begrepen, die het gevolg zijn van schending van deze verplichting.

Artikel 4: Verplichtingen Verwerker

4.1 De Verwerker zal ten aanzien van de in artikel 2 genoemde verwerkingen zorg dragen voor de naleving van de toepasselijke wet- en regelgeving, in het bijzonder de AVG.

4.2 De verplichtingen van de Verwerker die uit deze Overeenkomst voortvloeien, gelden ook voor degenen die persoonsgegevens verwerken onder het gezag van Verwerker, waaronder begrepen maar niet beperkt tot werknemers, in de ruimste zin van het woord.

4.3 Verwerker zal, voor zover dat binnen haar macht ligt, bijstand verlenen aan

Verwerkingsverantwoordelijke ten behoeve van het uitvoeren van PIA's in de zin van artikel 35 AVG.

Artikel 5: Inschakelen van derden of onderaannemers

5.1 Verwerker mag in het kader van deze Overeenkomst gebruik maken van door Verwerkingsverantwoordelijke goedgekeurde sub-verwerkers, bijvoorbeeld door de door Verwerkingsverantwoordelijke in het kader van gebruikmaking van de dienstverlening verwerkte persoonsgegevens, op te doen slaan op servers van derden.

5.2 Bijlage 1 bij deze Overeenkomst bevat een lijst met door Verwerkingsverantwoordelijke goedgekeurde sub-verwerkers. Indien Verwerker andere sub-verwerkers wenst in te zetten, zal zij Verwerkingsverantwoordelijke daarover voorafgaand per email informeren alsook de benodigde maatregelen treffen om ervoor te zorgen dat de sub-verwerkers dezelfde verplichtingen worden opgelegd als die waaraan Verwerker uit hoofde van de Overeenkomst en de wet jegens Verwerkingsverantwoordelijke moet voldoen. Indien Verwerkingsverantwoordelijke geen goedkeuring wenst te verlenen aan het inschakelen van de betreffende sub-verwerker(s), zal zij Verwerker hiervan uiterlijk binnen 2 weken na verzending van voornoemde e-mail schriftelijk of per e-mail op de hoogte stellen, in welk geval zowel Verwerker als Verwerkingsverantwoordelijke bevoegd zullen zijn de Licentieovereenkomst zonder enige verplichting tot vergoeding van schade te beëindigen per de datum waarop de beoogde sub-verwerker haar werkzaamheden voor Verwerker zal aanvangen.

5.3 Verwerker zorgt er in ieder geval voor dat deze derden schriftelijk ten minste dezelfde plichten op zich nemen als tussen Verwerkingsverantwoordelijke en Verwerker zijn overeengekomen.

5.4 Verwerker staat in voor een correcte naleving van de plichten uit deze Overeenkomst door deze derden en is bij fouten van deze derden zelf aansprakelijk voor alle schade alsof zij zelf de fout(en) heeft begaan, onverminderd het bepaalde in artikel 12 van deze Overeenkomst.

Artikel 6: Beveiliging

6.1 Verwerker zal de in Bijlage 2 beschreven technische en organisatorische maatregelen nemen met betrekking tot de te verrichten verwerkingen van persoonsgegevens, tegen verlies of tegen enige vorm van onrechtmatige verwerking (zoals onbevoegde kennisname, aantasting, wijziging of verstrekking van de persoonsgegevens).

6.2 Partijen stellen in hun onderlinge verhouding vast, dat de in artikel 6.1 genoemde beveiligingsmaatregelen een op het risico afgestemd passend beveiligingsniveau bieden. Verwerker staat jegens Verwerkingsverantwoordelijke niet in voor een resultaat maar staat er wel voor in dat de overeengekomen beveiligingsmaatregelen zijn genomen.

6.3 Verwerkingsverantwoordelijke stelt enkel persoonsgegevens aan Verwerker ter beschikking voor verwerking, indien zij zich ervan heeft verzekerd dat de vereiste beveiligingsmaatregelen zijn getroffen. Verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van de door Partijen afgesproken maatregelen.

Artikel 7: Melding beveiligingsincident en datalek

7.1 Om Verwerkingsverantwoordelijke in staat te stellen aan haar verplichtingen op grond van artikel 33 en 34 AVG te voldoen, stelt Verwerker de Verwerkingsverantwoordelijke onverwijld na ontdekking daarvan op de hoogte van ieder beveiligingsincident en ieder datalek. Onder beveiligingsincident wordt verstaan iedere inbreuk op de beveiliging zoals bedoeld in artikel 6 van deze Overeenkomst. Onder datalek wordt verstaan iedere inbreuk in verband met persoonsgegevens in de zin van artikel 4.12 AVG.

7.2 Verwerkingsverantwoordelijke is verantwoordelijk voor het melden van een datalek in de zin van artikel 33 en 34 AVG aan de toezichthouder en/of betrokkenen.

7.3 De melding van de Verwerker zoals bedoeld in artikel 7.1 bevat voor zover van toepassing in ieder geval:

- de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk

onder vermelding van de categorieën van betrokkenen en persoonsgegevens in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

- de naam en de contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
- de waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens;
- de maatregelen die de Verwerker heeft voorgesteld of genomen om de inbreuk in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

7.4 De Verwerker zal conform artikel 33.5 AVG alle datalekken documenteren, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Op verzoek zal de Verwerker de Verwerkingsverantwoordelijke hier inzage in verschaffen.

Artikel 8: Afhandeling verzoeken van betrokkenen

8.1 In het geval waarin een betrokkene een verzoek tot uitoefening van zijn/haar wettelijke rechten (in de zin van artikel 15 tot en met 22 AVG) richt aan Verwerker, mag Verwerker het verzoek van de betrokkene zelf afhandelen, en de Verwerkingsverantwoordelijke van de afhandeling op de hoogte stellen.

8.2 Verwerker mag de kosten voor de afhandeling van het verzoek wel doorbelasten aan Verwerkingsverantwoordelijke, nadat Verwerker hiervoor een offerte aan Verwerkingsverantwoordelijke heeft doen toekomen en Verwerkingsverantwoordelijke deze offerte heeft geaccordeerd.

Artikel 9: Controle op naleving beveiligingseisen

9.1 Verwerkingsverantwoordelijke heeft het recht om controles (audits) uit te laten voeren door een onafhankelijke derde die aan geheimhouding is gebonden ter controle van naleving van de beveiligingseisen, en alles dat daar direct verband mee houdt.

9.2 Deze audit mag op verzoek van Verwerkingsverantwoordelijke eens per jaar plaatsvinden en tevens bij een concreet vermoeden dat Verwerker zich niet houdt aan de verplichtingen die voortvloeien uit de Overeenkomst. Een audit zal slechts plaatsvinden op voorafgaande afspraak met Verwerker waarbij tevens de door Verwerkingsverantwoordelijke gewenste reikwijdte van de audit zo concreet mogelijk wordt vastgesteld, daar Verwerker vooraf dient te bepalen of de audit mogelijk systemen of diensten zal kunnen verstoren.

9.3 Verwerker zal aan de audit meewerken en alle voor de audit redelijkerwijs relevante informatie, inclusief ondersteunende gegevens zoals systeemlogs, en medewerkers zo tijdig mogelijk ter beschikking stellen.

9.4 De bevindingen naar aanleiding van de uitgevoerde audit zullen door Verwerker worden beoordeeld en kunnen, naar eigen goeddunken van Verwerker en op de wijze zoals Verwerker zelf bepaalt, worden doorgevoerd door Verwerker.

9.5 De kosten van de audit worden door Verwerkingsverantwoordelijke gedragen, tenzij de Verwerker zich niet houdt aan de verplichtingen die voortvloeien uit de Overeenkomst.

Artikel 10: Geheimhouding

10.1 Op alle persoonsgegevens die Verwerker van Verwerkingsverantwoordelijke ontvangt en/of zelf verzamelt in het kader van deze Overeenkomst, rust een geheimhoudingsplicht jegens derden. Verwerker zal deze informatie niet voor een ander doel gebruiken dan waarvoor zij deze heeft verkregen.

10.2 Deze geheimhoudingsplicht is niet van toepassing voor zover Verwerkingsverantwoordelijke

uitdrukkelijke toestemming heeft gegeven om de informatie aan derden te verschaffen, indien het verstrekken van de informatie aan derden logischerwijs noodzakelijk is gezien de aard van de verstrekte opdracht en de uitvoering van deze Overeenkomst, of indien er een wettelijke verplichting bestaat om de informatie aan een derde te verstrekken.

Artikel 11: Duur en beëindiging

11.1 Deze Overeenkomst geldt voor de duur van de tussen de partijen gesloten Licentieovereenkomst en bij gebreke daarvan, of in geval de verwerking op welke grond dan ook zou continueren na het eindigen van de Licentieovereenkomst, in ieder geval voor de duur van de samenwerking.

11.2 Zodra de Overeenkomst, om welke reden en op welke wijze dan ook, is beëindigd, zal Verwerker alle persoonsgegevens die bij haar aanwezig zijn wissen, tenzij opslag Unierechtelijk of lidstaatrechtelijk verplicht is.

Artikel 12: Aansprakelijkheid en vrijwaring

12.1 De aansprakelijkheid van Verwerker voor schade als gevolg van een toerekenbare tekortkoming in de nakoming van deze Overeenkomst, dan wel uit onrechtmatige daad of anderszins, is per gebeurtenis (een reeks opeenvolgende gebeurtenissen geldt als één gebeurtenis) beperkt tot een bedrag gelijk aan 5 (vijf) keer de op grond van de Licentieovereenkomst per jaar verschuldigde licentievergoeding, met een maximum van € 50.000,-.

12.2 In het geval Verwerker ten opzichte van Verwerkingsverantwoordelijke aansprakelijk is en de schade van Verwerkingsverantwoordelijke bestaat uit, of het gevolg is van een door een toezichthoudende autoriteit opgelegde last onder dwangsom of boete, is de aansprakelijkheid van Verwerker in afwijking van het bepaalde in artikel 12.1 beperkt tot een bedrag van € 100.000,-, hetgeen ook geldt voor enige bijdrageplicht overeenkomstig het bepaalde in Boek 6, Titel 1, Afdeling 2 van het Burgerlijk Wetboek, artikel 82 lid 5 AVG of enige andere wettelijke bepaling, in het geval Verwerker en Verwerkingsverantwoordelijke op grond van de AVG hoofdelijk aansprakelijk zijn voor een dergelijke dwangsom of boete.

12.3 Verwerker is in geen geval aansprakelijk voor indirecte schade of gevolgschade. Onder dergelijke schade wordt onder meer verstaan schade door gederfde winst, gemiste besparingen, verminderde goodwill, schade als gevolg bedrijfsstagnatie of vertraging en schade als gevolg van aanspraken van derden.

12.4 Verwerker is niet aansprakelijk voor schade die uitsluitend het gevolg is van door derden veroorzaakte defecten of storingen in software, hardware of netwerken, voor zover een dergelijk defect niet aan Verwerker bekend was op het moment van het ontstaan van de schade en Verwerker bovendien zelf alle maatregelen heeft getroffen die op grond van de AVG en artikel 6 van deze Verwerkersovereenkomst van haar mochten worden verwacht.

12.5 De in dit artikel bedoelde uitsluitingen en beperkingen komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van Verwerker.

12.6 Tenzij nakoming door Verwerker blijvend onmogelijk is, ontstaat de aansprakelijkheid van Verwerker wegens toerekenbare tekortkoming in de nakoming van de Overeenkomst slechts indien Verwerkingsverantwoordelijke de Verwerker onverwijld schriftelijk in gebreke stelt, waarbij een – gelet op de aard van de betreffende tekortkoming – redelijke termijn voor de zuivering van de tekortkoming wordt gesteld, en Verwerker ook na die termijn toerekenbaar blijft tekortschieten in de nakoming van haar verplichtingen. De ingebrekestelling dient een zo volledig en gedetailleerd mogelijke omschrijving van de tekortkoming te bevatten, opdat Verwerker in de gelegenheid wordt gesteld adequaat te reageren.

Artikel 13: Doorgifte van persoonsgegevens

13.1 Verwerker mag de persoonsgegevens verwerken in landen binnen de Europese Unie. Daarnaast mag Verwerker de persoonsgegevens ook ten behoeve van een juiste werking van de dienst(en) uit hoofde van de Licentieovereenkomst doorgeven naar een land buiten de Europese Unie, mits dit is

toegestaan op grond van de AVG.

Artikel 14: Toepasselijk recht en geschillenbeslechting

14.1 De Overeenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.

14.2 Alle geschillen, welke tussen Partijen mochten ontstaan in verband met de Overeenkomst, zullen exclusief worden voorgelegd aan de rechter die bevoegd is op grond van de Licentieovereenkomst en de daarop van toepassing zijnde algemene voorwaarden.

Bijlage 1 Omschrijving Persoonsgegevens, betrokkenen, doeleinden, sub-verwerkers en contactgegevens

De aard en het doel van de verwerking van persoonsgegevens

De aard van de verwerking waarvoor de Verwerker is ingeschakeld is:

- Het hosten van door de Verwerkingsverantwoordelijke opgemaakte en gepubliceerde Publicaties
- Het hosten van door de Verwerkingsverantwoordelijke gebruikte Formulieren

De doeleinden van een dergelijke verwerking en de doeleinden die daar redelijkerwijs aan verbonden zijn of die zijn bedongen onder verdere toestemming zijn:

- Het hosten van door de Verwerkingsverantwoordelijke opgemaakte en gepubliceerde Publicaties
- Het hosten van door de Verwerkingsverantwoordelijke gebruikte Formulieren

Betrokkenen

[een overzicht van categorieën van personen wiens persoonsgegevens worden verwerkt.]

Goedgekeurde sub-verwerkers

Name	**Location**	**Subprocessor status**	**Notes**
Rackspace	UK (London)	Application, database	
Amazon AWS	Germany (Frankfurt), London (UK)	Hotsite (DRP), screenshots (can include publication content)	
Google	Germany (Frankfurt)	Publishing, screenshots (can include publication content)	
Mandrill (Mailchimp)	United States	Submitted data (by visitors) to forms in publications	Opt-in on publication (can be turned off by account policy, contact us), certified for EU-US privacy shield
Logrocket	United States	Debugging/request logging on editor users (can include publication content)	Opt-in on forms/lead generation (customer support can retrigger opt-in), certified for EU-US privacy shield, Swiss-US privacy shield
MaxCDN / Stackpath	Global	Global CDN, e.g. local publication content hosting	Opt-out on publication (can be turned off by account policy, contact us)

Contactgegevens primair aanspreekpunt

Opdrachtgever als Verwerkingsverantwoordelijke:

Functie:

Naam:

E-mailadres:

Telefoonnummer:

Foleon B.V. als Verwerker:
Functie: Data Information Security Officer
Naam: Bart Brinkman
E-mailadres: bart.brinkman@foleon.com
Telefoonnummer: +31- 20303 28 22

Bijlage 2 technische en organisatorische beveiligingsmaatregelen

Beschrijving van de technische en organisatorische beveiligingsmaatregelen die door Verwerker overeenkomstig Artikel 6 zijn getroffen:

Foleon has focussed on protecting its customers' data and keeping up with the latest standards and industry best practices.

As a result, Foleon is compliant and/or certified with the following:

- **ISO 27001** - Foleon is independently certified by Kiwa N.V. for its Information Security
  - Note: Our primary hosting provider Rackspace is also ISO 27001 certified but also has received certifications for PCI DSS level 1 and SOC for its data centers.
- **OWASP** - As technology evolves, risks change. That's why our developers always comply with the latest OWASP secure coding standards.
- **GDPR** - At Foleon we value the privacy of you, your colleagues, and your customers and will always be transparent about any data that is used to improve your daily experience of the product. Read more about Foleon and GDPR compliance.

Our web-based application is set up using a **RESTful API** and an **AngularJS/ReactJS client** application. Foleon is entirely cloud-based and runs with a **multi-tenant single cluster code base**. Essentially, this means that every Foleon customer runs *exactly the same version of the platform.* All new features and improvements are developed, tested, and rolled-out through a **DTAP methodology**. This implements safe, separated environments for each development stage, and maximizes code quality once it goes into production. At that stage, it's available for all customers to use.

Once customers start using our platform, they create and upload content. To ensure data integrity, Foleon has a rigid back-up policy in place. Specifically, there are real-time backups (**replication or simple redundant disks**) in place over multiple instances and a daily (encrypted) backup to a separate environment. This includes all layers of the architecture, i.e. **Database, Application, and CDN**. All back-ups are encrypted and stored within the EU borders for 30 days.

To further increase availability and minimize service disruption, all critical services are designed as high-availability clusters.

Secure Access

Administrative access to our infrastructure is limited to trusted computers using **key authentication**. When data is transferred in our secured environment (e.g. the editor and any associated servers), connections are always encrypted **(TLS or SSH**).

For publications, Foleon-based hostnames (i.e. *.foleon.com) can only be requested using **https** (enforced by way of HSTS policies). Customer hostnames can optionally be secured with a **customer-provided TLS certificate.**

Users are authenticated using the **OAuth2 password grant** feature.

We ask our users, when they activate their account, to set their password with at least 1) one **digit character (0-9)**, and 2) a minimum **length of 8 characters**. Passwords in our database are stored hashed using the **bcrypt KDF**.

Under our **Information Security Policy**, access to personal and customer data is only granted to qualified personnel and always on a **need to know-basis.**

Secure Hosting

For our hosting needs, Foleon relies on the services of **Rackspace**. They are responsible for our **complete hardware setup** and are required to notify us of any security incident. They assist us in infrastructure deployment, configuration, maintenance, and various aspects of information security, including **Intrusion Detection System (IDS), Intrusion Prevention System (IPS)**, firewalls, patch management, health monitoring and alerting, and so on.

Firewalls (with a deny-by-default posture) protect the internal network zones and the network as a whole. **Vulnerability patch updates** are applied daily, with **backported security updates**.

Our systems are regularly **Pentested**.