Foleon Processor Agreement

20 May 2019

Article 1: Applicability

1.1 The use the services of Foleon pursuant to the licence agreement (the "Licence Agreement"), including by editing and publishing Magazines and/or using Forms, may constitute the processing of personal data within the meaning of Article 4.2 of the General Data Protection Regulation ("GDPR"). To the extent that you process personal data by using the services pursuant to the Licence Agreement and such processing is governed by the scope of the GDPR, the provisions of the present processor agreement (the "Agreement") will apply.

Article 2: Scope and Purposes

2.1 Foleon (the "Processor") undertakes to process personal data on your instructions subject to the provisions of this Agreement. You will hereinafter be referred to as the "Controller".

2.2 Given the nature of the services pursuant to the Licence Agreement, the Processor will not have any insight into the nature and type of personal data processed by the Processor for purposes of the services referred to in paragraph 1 or the categories of data subjects from whom they originate. The Controller instructs to process all categories of personal data and data subjects, to the extent processed by the Controller through the services of the Processor.

2.3 The Processor will process personal data solely for purposes of the Processor's storage on the Processor's servers or those of third parties engaged by the Processor, of the online magazines and/or forms created by or on behalf of the Processor. The Processor will not process the personal data for any purpose other than those established by the Controller. The Controller will notify the Processor of the purposes of processing to the extent not already stated in this Agreement.

2.4 The personal data to be processed on the instructions of the Controller will remain the property of the Controller and/or the relevant data subjects.

Article 3: General Obligations

3.1 The Processor will be responsible only for the processing of the personal data subject to this Agreement, in accordance with the instructions of the Controller and subject to the express ultimate responsibility of the Controller. In no event will the Processor be responsible for any other processing of personal data, in any event including but not limited to the collection of the personal data by the Controller, processing for any purposes other than those communicated by the Controller to the Processor, processing by any third parties and/or for any other purposes.

3.2 The Controller warrants that the contents and the use of, and the instruction to process, the personal data as referred to in this Agreement are not unlawful and do not infringe any rights of third parties, including the data subjects. The Controller will indemnify the Processor against any claims brought by third parties, including authorities, as a result of breach of this obligation.

Article 4: Processor Obligations

4.1 In respect of the processing referred to in article 2, the Processor will ensure compliance with the applicable laws and regulations, in particular the GDPR.

4.2 The Processor's obligations as ensuing from this Agreement will also extend to those processing personal data under the authority of the Processor, including but not limited to employees, in the broadest sense.

4.3 To the extent within its power, the Processor will lend its assistance to the Controller for purposes of implementation of DPIAs within the meaning of Article 35 GDPR.

Article 5: Engaging Third Parties or Subcontractors

5.1 For purposes of this Agreement, the Processor may engage sub-processors, by having the personal data processed by the Controller for purposes of use of the services stored on third-party servers.

5.2 Appendix 1 contains a list of sub-processors approved by the Controller. If the Processor wishes to use other sub-processors, the Processor will notify the Controller by email prior to the assignment of the sub-processors and take measures to ensure the same data protection obligations as set out in

this Agreement shall be imposed on those sub-processors. If the Controller objects to the assignment by the Processor of the relevant sub-processors(s), the Controller will inform the Processor of this in writing or by e-mail within 2 weeks after it has been notified by the Controller, in which case both the Processor and the Controller will be authorized to terminate the Licence Agreement as of the date on which the sub-processor will commence its work for the Processor, without any obligation to compensates costs or damages.

5.3 The Processor will ensure that such third parties undertake in writing at least the same obligations as agreed between the Controller and the Processor.

5.4 The Processor warrants proper compliance with the obligations under this Agreement by any such third parties and, in the event of errors by such third parties, will be liable for any and all damage as if it had committed such error or errors itself, the Processor's liability being limited to that provided for in article 12 of this Agreement.

Article 6: Security

6.1 The Processor will endeavour to take the appropriate technical and organisational measures, as described in Appendix 2, to protect the personal data to be processed against loss or any form of unlawful processing (such as unauthorised access, impairment, modification or disclosure of the personal data).

6.2 The Parties establish that the security measures referred to in Article 6.1, are deemed appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The Processor does not guarantee that the security is effective under all circumstances. The Processor does guarantee that the agreed measures have been taken.

6.3 The Controller will make personal data available to the Processor for processing only if it has ascertained that the required security measures have been taken. The Controller will be responsible for compliance with the measures agreed between the Parties.

Article 7: Notification of Security Incident of Data Leak

7.1 In order to enable the Controller to perform its obligations under Articles 33 and 34 GDPR, the Processor will notify the Controller of any security incident or any data leak promptly upon discovery. A security incident will be understood as any breach of security within the meaning of article 6 of this Agreement. A data leak will be understood as any personal data breach within the meaning of Article 4.12 GDPR.

7.2 The Controller will be responsible for notification of the supervisory authority and/or any data subjects in the event of any data leak within the meaning of Articles 33 and 34 GDPR.

7.3 The notification by the Processor as referred to in article 7.1 will in any event include, to the extent applicable:

- the nature of the personal data breach, where possible stating the categories of data subjects and personal data involved and an estimate of the number of data subjects and personal data records involved;
- the name and contact details of the data protection officer or another contact for more information;
- the likely consequences of the personal data breach;
- the measures proposed or taken by the Processor in order to address the personal data breach, including, if the situation arises, the measures to mitigate any adverse effects thereof.

7.4 The Processor will document any data leaks in accordance with Article 33.5 comprising the facts relating to the personal data breach, its effects and the remedial action taken. The Processor will give the Controller access to such documentation on request.

Article 8: Handling requests from data subjects

8.1 In the event that a data subject submits a request to exercise their statutory rights (within the meaning of Articles 15 to 22 inclusive of the GDPR) to the Processor, the Processor may handle the request from the data subject itself subject to notification of the Controller of such handling.

8.2 The Processor may, however, pass on any costs of handling the request to the Controller, after the Processor has forwarded a quotation for this to the Controller and the Controller has approved this quotation.

Article 9: Monitoring compliance with security requirements

9.1 The Controller will have the right to instruct a third party, subject to a confidentiality obligation, to conduct audits in respect of compliance with the security requirements and any related matters.

9.2 Such audits may be conducted at the request of the Controller once per year, as well as in the event of suspected abuse of personal data. An audit will be conducted only after scheduling an appointment with the Processor, the Controller determining the desired scope of the audit in as concrete terms as possible, as the Processor must determine in advance whether the audit may disrupt any systems or services.

9.3 The Processor will lend its cooperation in the audit and provide all such information, including supporting data, such as system logs, and resources, as may be reasonably relevant to the audit as soon as possible.

9.4 The findings of the audit conducted will be reviewed by the Processor and may, at the Processor's discretion and in such a manner as the Processor may determine, be implemented by the Processor.

9.5 The costs of the audit will be payable by the Controller, unless the Processor is in material breach of its obligations under this Agreement.

Article 10: Confidentiality

10.1 Any and all personal data received by the Processor from the Controller and/or collected by the Processor itself for purposes of this Agreement must be kept confidential vis-à-vis third parties. The Processor will not use such information for any purposes other than the purpose for which it was obtained.

10.2 This confidentiality obligation will not apply to the extent that the Controller has granted its express consent to disclosure of the information to third parties, if disclosure of the information to third parties is logically necessary given the nature of the instruction given and performance of this Agreement, or in the event of a statutory duty to disclose the information to third parties.

Article 11: Term and termination

11.1 This Agreement will continue in effect for the term of the Licence Agreement and, in the absence thereof, or in the event that, for any reason whatsoever, the processing should continue after termination of the Licence Agreement, in any event for the duration of the partnership.

11.2 Upon termination of the Agreement, for any reason and in any manner whatsoever, the Processor will erase any and all personal data in its possession, unless storage is required pursuant to Union or Member State law.

Article 12: Liability and indemnification

12.1 Any liability of the Processor due to an attributable shortcoming under this Agreement or an unlawful act or otherwise, will be limited to 5 (five) times the amount owed by the Controller under the Licence Agreement in respect of licence costs for one year, with a maximum of EUR 50.000,--.

12.2 If the Processor is liable towards the Controller and if the damage suffered by the Controller consists of, or is the result of a penalty imposed by a data protection supervisory authority which is collected from the Controller as a result of the Processor failing to comply with this Agreement, the Processor’s liability is, in derogation from the provisions of Article 12.1, limited to an amount of EUR 100.000,--. This also applies to any obligation to contribute in accordance with the provisions of Book 6, Title 2, Section 2 of the Dutch Civil Code Article 82, paragraph 5 of the DGPR or any other

statutory provision, in the event that the Processor and the Controller are jointly and severally liable for such a penalty pursuant to the GDPR.

12.3 In no event will the Processor be liable to compensate any indirect and/or consequential damage suffered by the Controller. Indirect and/or consequential loss will include, but will not be limited to, all and any damage or loss that is the result of any loss of profits, loss of savings, reputational damage or loss of goodwill, damage due to interruption of the business of the Controller or due to loss or temporary non-availability of data, and damages resulting from claims of any third party on the Controller.

12.4 The Processor is never liable for damage that is the result of defects caused by third parties or malfunctions in software, hardware or networks, insofar as such a defect was not known to the Processor at the time of the occurrence of the damage and the Processor has taken all measures it should have taken based the GDPR and article 6 of this Agreement.

12.5 Any exclusion and limitation of liability in shall not apply if and insofar as the damage is the result of intent and/or gross negligence of the Processor.

12.6 Unless compliance by the Processor is permanently impossible, the liability of the Processor for an imputable failure to comply with the Agreement is subject to the Controller giving the Processor immediate and written notice of default, specifying a reasonable period - given the nature of the failure - to remedy the failure and the Processor continuing to imputably fail in the fulfilment of his obligations after that term. In order to allow the Processor to respond effectively, the notice of default must contain a description of the failure that is as accurate and detailed as possible.

Article 13: Transfer of personal data

13.1 The Processor may process the personal data in countries within the European Union. In addition, the Processor may also transfer the personal data to a country outside the European Union for purposes of proper performance of the service or services pursuant to the Licence Agreement, provided that this is permitted by the GDPR.

Article 14: Applicable law and dispute resolution

14.1 The Agreement and its performance will be governed by the laws of the Netherlands.

14.2 Any disputes that may arise between the Parties in connection with the Agreement will be submitted exclusively to the court that has jurisdiction pursuant to the Licence Agreement and the applicable general conditions.

Appendix 1 Description of Personal Data, data subjects, data processing purposes, sub-processors and contact details

The nature and purpose of the processing of personal data

The nature of the processing for which the processor is involved is:

- Hosting of Publications prepared and published by the Controller
- Hosting of Forms used by the Controller

The purposes of such processing and the purposes that are reasonably attached to it or that are stipulated with further permission are:

- Hosting of Publications prepared and published by the Controller
- Hosting of Forms used by the Controller

Data subjects

[A list of categories of data subjects whose personal data is being processed.]

Approved sub-processors

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)

Contact details

Client as Controller:
Function:
Name:
E-mail address:
Phone number:

Foleon B.V. as Processor:
Function: Chief Information Security Officer
Name: Bart Brinkman
E-mail address: bart.brinkman@foleon.com
Phone number: +31 20-3032822

Appendix 2 Technical and organizational security measures

Description of the technical and organizational security measures taken by the Processor in accordance with article 6:

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**.