DPA Appendix 1: Foleon Data Processing Agreement (this "DPA")

Last Modified: 1st of August 2023

1. Applicability

1.1. This DPA supplements that certain Master Services Agreement (the "MSA") entered into by Foleon B.V. ("Foleon" or "Processor") and [INSERT NAME] (the "Customer" or "you") dated [INSERT DATE], as such may be amended by the Parties from time to time pursuant to the terms thereof. Foleon's performances of the Services, including the editing and publishing of magazines and/or using forms (the "Services"), may constitute the processing of personal data ("Personal Data") within the meaning of Article 4.2 of the General Data Protection Regulation ("GDPR"). Such processing of Personal Data shall be governed by the GDPR, the Dutch GDPR Implementation Act ('Uitvoeringswet AVG') and other applicable national implementation laws relating to the GDPR (together with the applicable data privacy laws are hereinafter referred to as the "Data Privacy Laws") and the terms of this DPA.

1.2. The terms of this DPA are incorporated in the MSA by reference and shall form an integral part thereof. Capitalized terms not defined herein shall have the meaning assigned to them in the MSA. This DPA applies only to the Processor's processing of Personal Data for the nature, purposes and duration set forth in Appendix I.

2. Scope and Purposes

2.1. Foleon (the "Processor") undertakes to process personal data on your instructions subject to the provisions of this DPA. For the purposes of this DPA, the Controller is the Party responsible for determining the purposes of processing Client Data. You will hereinafter be referred to as the "Controller".

2.2. Given the nature of the Services, the Processor will not have any insight into the nature and type of Personal Data processed by the Processor for purposes of performing the Services or the categories of data subjects from whom they originate.

2.3. The Controller instructs Processor to process, retain, use or disclose Personal Data solely for the specific business purposes and Services set forth in Appendix 1 or for such other business purposes as permitted by the Data Privacy Laws or as may be agreed by the Parties from time to time. The Controller shall only disclose Personal Data to the Processor for the limited and specified business purposes set forth in Appendix I.

2.4. The ownership of the Personal Data shall be as set forth in Section 6 of the MSA.

3. General Obligations

3.1. The Processor will be responsible only for the processing of the Personal Data subject to this DPA, in accordance with the instructions of the Controller and subject to the express ultimate responsibility of the Controller. The Processor shall be prohibited from selling or sharing Personal Data it receives from, or on behalf of, the Controller except to sub-processors or subcontractors as set forth in Section 5 of this DPA.

3.2. In no event will the Processor be responsible or liable for any other processing of Personal Data other than those in relation to the Services and in accordance with the terms of this DPA. Without limiting the foregoing, the Processor shall not be responsible or liable for the collection or processing of the Personal Data by the Controller, processing for any purposes other than those communicated by the Controller to the Processor under the MSA, processing by any third parties and/or for any other purposes.

3.3. In addition to the Controller's representations and warranties with respect to the Customer Data as set forth in Section 5 of the MSA and the Controller's indemnification obligations related thereto as set forth in Section 16 of the MSA, the Controller hereby represents and warrants that the retention, collection, use, disclosure of Personal Data and the Controller's instructions for processing of the Personal Data do not violate any Data Privacy Laws. The Controller hereby indemnifies, defends, and holds the Processor, its affiliates, their respective directors, officers, employees and agents from and against any third-party claims and liabilities (including penalties, courses of actions and claims from government authorities) to the extent resulting from the Controller's breach of such representations and warranties.

3.4. The Controller shall inform the Processor of any consumer request made pursuant to the applicable Data Privacy Laws that the Processor must comply with, and provide the information necessary for the Processor to comply with the request.

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. To the extent commercially reasonable, the Processor will lend its assistance to the Controller for purposes of implementation of a Data Protection Impact Assessment ("DPIA") within the meaning of Article 35 GDPR.

5. Engaging Sub-processors or Subcontractors

5.1. For purposes of this DPA, the Processor may engage sub-processors or subcontractors, to process the Personal Data and use commercially reasonable efforts to enter into a contract with such sub-processors or subcontractors that complies with the applicable Data Privacy Laws and the terms of this DPA.

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 DPA shall be imposed on such new sub-processors. If the Controller objects to the assignment by the Processor of any new sub-processors(s) not listed in Appendix 1, 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 either the Processor or the Controller may terminate the MSA effective as of the date on which the sub-processor will commence its work for the Processor, without any obligation of the Processor to the Controller to compensate costs or damages. Nothing in this DPA shall restrict the Parties' termination rights under Section 12 of the MSA.

5.3. The Processor will ensure that such third parties undertake 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 DPA by any such third parties and, in the event of errors by such third parties, will be liable for 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 DPA.

6. Security

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

6.2. The Parties hereby acknowledge and agree 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.

7. Notification of Security Incident of Data Breach

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 breach without undue delay upon discovery. A security incident will be understood as any breach of security within the meaning of article 6 of this DPA. A data breach 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 breach 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 breaches in accordance with Article 33.5 GDPR 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 upon reasonable request.

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), the Controller must inform the Processor of any such request made pursuant to the Data Privacy Laws. If the data subject submits a

request to the Processor, the Processor shall notify the Controller about such request and coordinate the response with the Controller to the extent such coordination or disclosure of the request is permissible under the applicable Data Privacy Law. If required by the applicable Data Privacy Law, the Processor may handle the request from the data subject itself subject to any conditions set forth in the applicable Data Privacy Law.

8.2. To the extent permissible under the applicable Data Privacy Law, the Processor may directly pass on to the Controller any costs or all costs incurred by the Processor because of the Processor's handling of the data subject's request or request a reimbursement of advanced costs from the Controller. Controller agrees to pay to the Processor such costs promptly upon receipt of Processor's request for payment.

9. Monitoring compliance with security requirements

9.1. The Controller will have the right to instruct a qualified and independent third party, subject to a confidentiality obligation, to conduct audits in respect of the Processor's compliance with this DPA.

9.2. Such audits may be conducted at the request of the Controller once per twelve (12) months during the term of the MSA, as well as in the event the Controller has reason to believe (with adequate written documentation) that the Processor has breached the terms of this DPA. An audit will be conducted only with reasonable advance notice to the Processor in writing and after agreeing on an appointment with the Processor. In the written notice, the Controller shall determine 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. The Processor shall only be required to agree to the requested scope of the audit to the extent the audit is necessary to review the Processor's compliance with this DPA.

9.3. To the extent commercially reasonable to the Processor, the Processor will cooperate in good faith with 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. If the audit's findings allege a material breach of this DPA by the Processor, the Processor may dispute such claim of material breach by engaging an independent, qualified third party to conduct a second audit. In the event the Processor does not dispute the material breach, or the second audit reveals a material breach of this DPA by the Processor, the Processor shall, within a reasonable time and as permissible under the applicable Data Privacy Law, cure such material breach within a reasonable time at the Processor's sole expense.

9.5. The costs of the audit will be paid by the Controller, unless (i) such audit reveals that the Processor is in material breach of the obligations under this DPA (as determined pursuant to Section 9.4 and (ii) the Processor has not disputed such material breach or (iii) failed to cure such material breach within a reasonable time after the Processor was notified by the Controller about such material breach.

10. Confidentiality

10.1. All Personal Data received by the Processor from the Controller and/or collected by the Processor itself for purposes of this DPA must be kept confidential vis-à-vis third parties. The

Processor's confidentiality obligations (including the applicable exemptions) under Section 13 of the MSA shall apply to all Personal Data processed by the Processor under this MSA.

10.2. Without limiting the exemptions under Section 13.2 of the MSA, the following shall be exempt from the Processor's confidentiality obligations under the MSA or this DPA: (i) Personal Data for which the Controller has granted the Processor's express consent for its disclosure to third parties, (ii) the disclosure of the Personal Data to third parties to the extent necessary (as determined by the Processor) given the nature of the Controller's instruction given to the Processor, and/or (iii) disclosure or processing of Personal Data necessary for the Processor's performance of the Services or its other obligations under the MSA or this DPA.

11. Term and termination

11.1. This DPA will continue in effect for the term of the MSA and, in the absence thereof, or in the event that, for any reason whatsoever, the processing should continue after termination of the MSA, in any event for as long as the Processor processes Personal Data on behalf of the Controller under the MSA.

11.2. Upon the expiration or termination of the DPA, for any reason and in any manner whatsoever, the Processor will erase all Personal Data in its possession within such period as required by the applicable Data Privacy Law, unless storage is required or permissible pursuant to the applicable Data Privacy Law.

12. Liability and indemnification

12.1. The provisions limiting the Processor's liability under the MSA (including but not limited to Sections 18 and 19) shall apply to any liability of the Processor under this DPA.

12.2. The indemnification obligations by the Parties set forth under Section 16 of the MSA together with the conditions set forth therein shall apply to any third-party claims arising from the respective Party's breach of this DPA or the applicable Data Privacy Law.

13. Other Terms of the MSA

13.1. The Parties acknowledge and agree that all other terms of the MSA even if not explicitly referred to in this DPA shall apply, including but not limited to the terms with respect to Customer Data (Section 6), Personal Data (Section 7), General Terms (Section 20) and the Order of Precedence (Section 21).

14. Transfer of Personal Data

14.1. The Controller hereby agrees that the Processor may process the Personal Data in the United States and 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 the Processor's performance of the Services; to the extent such transfer is permitted by the applicable Data Privacy Law.

15. Changes to Applicable Data Privacy Laws

15.1. The Parties agree to cooperate in good faith to enter into additional or modified terms to address any modifications, amendments, or updates to the applicable Data Privacy Laws and their regulations.

16. Applicable law and Dispute Resolution

16.1. The laws of the Netherlands will govern the DPA and its performance.

16.2. Any disputes that may arise between the Parties in connection with the DPA will be submitted exclusively to the court that has jurisdiction pursuant to the MSA.

Foleon Data Processing Agreement: 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 Foleon Docs 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 Foleon Docs 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 /subcontractors

Name	Address	Jurisdiction	Sub-processor /subcontractor status	Notes
Amazon AWS	Amazon Web Services EMEA SARL Johanna Westerdijkplein 1 2521 EN Den Haag Netherlands	EU (Germany)	Hotsite (DRP), screenshots (can include Foleon Doc content)	Hosting Provider
Google Cloud Platform (GCP)	Google Ireland Limited Google Building Gordon House, Barrow St, Dublin 4 Ireland	EU (Netherlands)	Application, database	Hosting Provider
Google Cloud Platform (GCP)	Google Ireland Limited Google Building Gordon House, Barrow St, Dublin 4 Ireland	EU (Germany)	Publishing, screenshots (can include Foleon Doc content)	Hosting Provider
Amazon AWS CloudFront	Amazon Web Services EMEA SARL Johanna Westerdijkplein 1 2521 EN Den Haag Netherlands	Global	Global CDN, e.g. local Foleon Doc content hosting	Opt-out on Foleon Doc (can be turned off by account policy, contact us)
Mandrill (Mailchimp)	The Rocket Science Group LLC	United States	Submitted data (by visitors) to	Opt-in on Foleon Doc

	675 Ponce de Leon Avenue Northeast, Suite 5000 Atlanta, GA 30308 United States		forms in Foleon Doc	(can be turned off by account policy, contact us), usage of services can be performed through established SCC's (client approval and opt-in).
Northpass	Northpass, Inc 6th Upper Pond Road, Parsippany, New Jersey	United States	Data is only processed for the purpose of providing LMS capabilities and services.	Customers added to the platform known as Foleon Academy voluntarily or by email invite. Usage of services can be performed through established SCC's.

Contact details

Customer as Controller:

Function:

Name:

E-mail address:

Phone number:

Foleon B.V. as Processor:

Function: Information Security Officer

Name: Bart Brinkman

E-mail address: bart.brinkman@foleon.com

Phone number: +31 20-3032822

Foleon Processing Agreement : Appendix 2

Technical and organizational security measures

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

Foleon has focused 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 providers Rackspace and GCP are also ISO 27001 certified and have received certifications for PCI DSS level 1 and attestation for SOC2 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 **Angular/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 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

We utilize an Infrastructure as Code (IaC) process. This gives us a good overview on our cluster and security rules. In this container-based architecture we have rules in place for firewalls, patch/package management, vulnerability scans, 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**.