Data Processing Agreement

4MATION

5/27/21

Version d.d. 27 May 2021

DATA PROCESSING AGREEMENT

PARTIES:

[Full legal name counter party], a private company with limited liability incorporated under the laws of [the Netherlands], having its corporate seat at [city] and its principal place of business at [full address], registered in the commercial register under number [●], hereinafter referred to as the "Customer", represented by [name, position];

and

[Plat4mation BV] a private company with limited liability incorporated under the laws of the Netherlands, having its corporate seat at [Utrecht] and its principal place of business at [Arthur van Schendelstraat 650, 3511 MJ Utrecht], registered in the commercial register under number [58858334], hereinafter referred to as "4Mation", represented by [name, position].

The Customer and 4Mation are sometimes herein collectively referred to as the "Parties" and individually as a "Party".

WHEREAS:

A. 4Mation is part of the 4Mation Group and is an Elite ServiceNow Partner dedicated to delivering world-class products and services for the ServiceNow platform;
B. The Customer is [insert brief description of activities Customer];
C. 4Mation and Customer entered into a Professional Services Agreement under which 4Mation provides to the Customer certain services as described therein.
D. In executing the Professional Services Agreement, Customer will provide certain personal data to 4Mation which 4Mation will process;
E. The Customer needs to comply with the Data Protection Laws and therefore wishes to enter into this Data Processing Agreement with 4Mation;

NOW, THEREFORE, IT IS HEREBY AGREED AS FOLLOWS:

1. DEFINITIONS

1.1 "Affiliates" means any person or entity directly or indirectly Controlling, Controlled by or under common Control with a party to the Agreement, where "Control" means the legal power to direct or cause the direction of the general management of the company, partnership, or other legal entity.
1.2 "Agreement" means the Professional Services Agreement between 4Mation and Customer.
1.3 "Data Controller" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of Processing of Personal Data. For purposes of this DPA, Data Controller is Customer and, where applicable, its Affiliates whose Personal Data is Processed under the Agreement.
1.4 "Data Processor" means the natural or legal person, public authority, agency, or other body which Processes Personal Data on behalf of the Data Controller. For purposes of this DPA, Data Processor is the 4Mation entity that is a party to the Agreement.
1.5 "Data Protection Laws" means all applicable laws and regulations regarding the Processing of Personal Data and includes GDPR.
1.6 "Data Subject" means an identified or identifiable natural person.
1.7 "DPA" means this Data Protection Agreement.
1.8 "GDPR" means the European Union's General Data Protection Regulation (2016/679).
1.9 "Instructions" means Data Controller's documented data Processing instructions issued to Data Processor in compliance with this DPA.
1.10 "Personal Data" means any information relating to a Data Subject that 4Mation processes for and on behalf of Customer as described in Appendix 1 to this DPA while performing the Services under the Agreement..
1.11 "Process" or "Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure or destruction.
1.12 "Security Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
1.13 "Security Policy Framework" means the framework that Data Processor has in place providing appropriate technical and organizational safeguards to protect the security, confidentiality, and integrity of Customer Data, including any Personal Data contained therein and that is enclosed as Appendix 2. The Security Policy Framework is designed to protect Customer Data from loss, alteration, unauthorized access, acquisition, use, disclosure, or accidental or unlawful destruction.
1.14 "Services" means the professional services provided by 4Mation under the Agreement.
1.15 "Sub-Processor" means any legal person or entity engaged in the Processing of Personal Data by Data Processor.
1.16 "Supervisory Authority" means an independent public authority established in accordance with the Data Protection Laws.

2. SCOPE OF THE PROCESSING

2.1 COMMISSIONED PROCESSOR. Data Controller appoints Data Processor to Process Personal Data on behalf of Data Controller to the extent necessary to provide the Services and in accordance with the Instructions.
2.2 INSTRUCTIONS. The Agreement constitutes Data Controller's written Instructions to Data Processor for Processing of Personal Data. Data Controller may issue additional or alternate Instructions provided that such Instructions are: (a) consistent with the purpose and the scope of the Agreement; and (b) confirmed in writing by Data Controller. For the avoidance of doubt, Data Controller shall not use additional or alternate Instructions to alter the scope of the Agreement. Data

Controller is responsible for ensuring its Instructions to Data Processor comply with Data Protection Laws.
2.3 NATURE, SCOPE AND PURPOSE OF THE PROCESSING. Data Processor shall only Process Personal Data in accordance with Data Controller's Instructions and to the extent necessary for providing the Services.
2.4 CATEGORIES OF PERSONAL DATA AND CATEGORIES OF DATA SUBJECTS. Data Controller may submit Personal Data as Customer Data, the extent of which is determined and controlled by Data Controller in its sole discretion and as further described in Appendix 1.

3. DATA CONTROLLER

3.1 COMPLIANCE WITH DATA PROTECTION LAWS. Data Controller shall comply with all its obligations under Data Protection Laws when Processing Personal Data.
3.2 SECURITY RISK ASSESSMENT. Data Controller agrees that in accordance with Data Protection Laws and before submitting any Personal Data to Data Processor under the Agreement, Data Controller will perform an appropriate risk assessment to determine whether the Security Policy Framework provides an adequate level of security, taking into account the nature, scope, context and purposes of the processing, the risks associated with the Personal Data and the applicable Data Protection Laws. Data Processor shall provide Data Controller reasonable assistance by providing Data Controller with information requested by Data Controller to conduct Data Controller's security risk assessment. Data Controller is solely responsible for determining the adequacy of the Security Policy Framework in relation to the Personal Data Processed.
3.3 CUSTOMER'S AFFILIATES. The obligations of Data Processor set forth herein will extend to Data Controller Affiliates to which 4Mation provides the Services or whose Personal Data is Processed within the Services, subject to the following conditions:
3.3.1. COMPLIANCE. Customer shall at all times be liable for its Affiliates' compliance with this DPA and all acts and omissions by a Data Controller Affiliate are considered acts and omissions of Customer;
3.3.2. CLAIMS. Data Controller Affiliates will not bring a claim directly against Data Processor. In the event a Data Controller Affiliate wishes to assert a valid legal action, suit, claim or proceeding against Data Processor (a "Data Controller Affiliate Claim"): (i) Customer must bring such Data Controller Affiliate Claim directly against Data Processor on behalf of such Data Controller Affiliate, unless Data Protection Laws require that Data Controller Affiliate be party to such Data Controller Affiliate Claim; and (ii) all Data Controller Affiliate Claims will be considered claims made by Customer and are at all times subject to any aggregate limitation of liability set forth in the DPA.
3.4 COMMUNICATION. Unless otherwise provided in this DPA, all requests, notices, cooperation, and communication, including Instructions issued or required under this DPA (collectively, "Communication"), must be in writing and between Customer and 4Mation only and Customer shall inform the applicable Data Controller Affiliate of any Communication from 4Mation pursuant to this DPA. Customer shall be solely responsible for ensuring that any Communications (including Instructions) it provides to 4Mation relating to Personal Data for which a Customer Affiliate is Data Controller reflect the relevant Customer Affiliate's intentions.

4. DATA PROCESSOR

4.1 DATA CONTROLLER'S INSTRUCTIONS. Data Processor will have no liability for any harm or damages resulting from Data Processor's compliance with Instructions received from Data Controller. Where Data Processor believes that compliance with Data Controller's Instructions could result in a violation of Data Protection Laws, Data Processor shall promptly notify Data Controller thereof. Data Controller acknowledges that Data Processor is reliant on Data Controller's representations regarding the extent to which Data Controller is entitled to Process Personal Data.
4.2 DATA PROCESSOR PERSONNEL. Access to Personal Data by Data Processor will be limited to personnel who require such access to perform Data Processor's obligations under the Agreement and who are bound by appropriate obligations to maintain the confidentiality of such Personal Data.
4.3 DATA SECURITY MEASURES. Without prejudice to Data Controller's security risk assessment obligations under Section 3.2 (Security Risk Assessment) above, Data Processor shall maintain the Security Policy Framework. Data Processor regularly tests, assess and evaluates the effectiveness of its Security Policy Framework and may periodically review and update the Security Policy Framework to address new and evolving security technologies, changes to industry standard practices, and changing security threats.
4.4 DELETION OF PERSONAL DATA. Upon termination or expiration of the Agreement, Data Processor shall return to Customer and delete Customer Data, including Personal Data contained therein.
4.5 DATA PROTECTION IMPACT ASSESSMENTS (DPIA). Data Processor will, on request, provide Data Controller with reasonable information required to fulfill Data Controller's obligations under GDPR to carry out data protection impact assessments, if any, for Processing of Personal Data within the Subscription Service.
4.7 PRIOR CONSULTATION. Data Processor shall provide reasonable assistance (at Data Controller's expense) in connection with any prior consultation Data Controller is required to undertake with a Supervisory Authority under Data Protection Laws with respect to Processing of Personal Data under the Agreement.
4.8 DATA PROCESSOR ASSISTANCE. Data Processor will assist Data Controller in ensuring compliance with Data Controller's obligations pursuant to Articles 32 to 36 of GDPR taking into account the nature of Processing by providing Data Controller with reasonable information requested pursuant to the terms of this DPA, including information required to conduct Data Controller's security risk assessment and respond to Data Subject Requests (defined below). For clarity, Data Controller is solely responsible for carrying out its obligations under GDPR and this DPA. Data Processor shall not undertake any task that can be performed by Data Controller.
4.9 DATA PROTECTION CONTACT. 4Mation and its Sub-Processor Affiliates (defined below) will maintain a dedicated data protection team to respond to data

protection inquiries throughout the duration of this DPA and can be contacted at: security@plat4mation.com.

5. REQUESTS MADE FROM DATA SUBJECTS AND AUTHORITIES

5.1 REQUESTS FROM DATA SUBJECTS. During the Services under the agreement, Data Processor shall provide Data Controller with the ability to access, correct, rectify, erase, or block Personal Data, or to transfer or port such Personal Data, as may be required under Data Protection Laws (collectively, "Data Subject Requests").

5.2 RESPONSES. Data Controller will be solely responsible for responding to any Data Subject Requests, provided that Data Processor shall reasonably cooperate with the Data Controller to respond to Data Subject Requests to the extent Data Controller is unable to fulfill such Data Subject Requests using the functionality in the Subscription Service. Data Processor will instruct the Data Subject to contact the Customer in the event Data Processor receives a Data Subject Request directly.

5.3 REQUESTS FROM AUTHORITIES. In the case of a notice, audit, inquiry, or investigation by a government body, Supervisory Authority, or law enforcement agency regarding the Processing of Personal Data, Data Processor shall promptly notify Data Controller unless prohibited by applicable law. Data Controller shall keep records of the Personal Data Processed by Data Processor and shall cooperate and provide all necessary information to Data Processor in the event Data Processor is required to produce such information to a Supervisory Authority.

5.4 COOPERATION WITH SUPERVISORY AUTHORITIES. In accordance with Data Protection Laws, Data Controller and Data Processor shall cooperate, on request, with a Supervisory Authority in the performance of such Supervisory Authority's task.

6. SECURITY BREACH NOTIFICATION

6.1 NOTIFICATION. Data Processor will report to Data Controller any Security Breach that it becomes aware of without undue delay, but in any event with 48 hours, following determination by 4Mation that a Security Breach has occurred. Together with the notification, 4Mation shall provide to Customer the form as set out in Appendix 3 to the DPA, filled in as much as possible.

6.2 REPORT. The initial report will be made to Data Controller's security or privacy contact(s) designated by Customer in this DPA (or if no such contact(s) are designated, to the primary contact designated by Customer). As information is collected or otherwise becomes available, Data Processor shall provide without undue delay any further information regarding the nature and consequences of the Security Breach to allow Data Controller to notify relevant parties, including affected Data Subjects, government agencies and Supervisory Authorities in accordance with Data Protection Laws. The report will include the name and contact information of the Data Processor contact from whom additional information may be obtained. Data Processor shall inform Customer of the measures that it will adopt to mitigate the cause of the Security Breach and to prevent future Security Breaches.

6.3 DATA CONTROLLER OBLIGATIONS. Data Controller will cooperate with Data Processor in maintaining accurate contact information and by providing any information that is reasonably requested to resolve any security incident, including any Security Breaches, identify its root cause(s), and prevent a recurrence. Data Controller is solely responsible for determining whether to notify the relevant Supervisory Authority or any other regulatory authorities and impacted Data Subjects and for providing such notice.

7. CUSTOMER MONITORING RIGHTS

7.1 AUDIT. In order to determine whether Data Processor complies with the provisions of this Data Processing Agreement, Data Controller shall have the right, no more than once per year, and taking into account a reasonable notice period of at least 2 weeks, to perform an audit ("Audit") of the Data Processor. The Audit will be performed by the Data Controller or an independent third party appointed by the Data Controller, provided that such third party shall enter into written obligations of confidentiality directly with Data Processor. The Audit will be performed at a mutually agreed date, no longer than two months after the initial request of the Data Controller. Data Processor shall, on the request of the auditor, provide access to its facilities, policies and documentation, reasonably necessary for the purpose of the Audit. Data Processor reserves the right to refuse to provide Customer (or its representatives) with any information which would pose a security risk to Data Processor or its customers, or which Data Processor is prohibited to provide or disclose under applicable law or contractual obligations. Such Audit shall include a written summary report of any assessment performed by an independent third-party of Data Processor's information security management system supporting the professional services against the objectives stated in ISO 27001

7.2 OUTPUT. Upon completion of the Audit, Data Processor and Customer may schedule a mutually convenient time to discuss the output of the Audit. In the event that the results of the Audit show that the Data Processor has not met its obligations under this Data Processing Agreement, Data Processor will implement Customer's reasonably suggested improvements as noted in the Audit to improve Data Processor's Security Policy Framework. The Audit and the results derived therefrom are Confidential Information of Data Processor.

7.3 EXPENSES. Any expenses incurred by Data Controller in connection with the Audit, including the costs of the independent third party performing the Audit, shall be borne exclusively by Data Controller. Only in the event that the Audit shows that the Data Processor has materially not met its obligations under this Data Processing Agreement, and the not meeting of its obligations is attributable to Data Processor, will the costs of the auditor be borne by the Data Processor.

8. SUB-PROCESSORS

8.1 USE OF SUB-PROCESSORS. 4Mation shall not engage a Sub-Processor, without the prior written consent of the Data Controller.

8.2 APPROVAL OF SUB-PROCESSORS Prior to Data Processor engaging a Sub-Processor, Data Processor shall: (a) ask Data Controller by email to Customer's designated contact(s) for its prior written approval and (b) ensure that such Sub-Processor has entered into a written agreement with Data Processor (or the relevant Data Processor

Affiliate) requiring that the Sub-Processor abide by terms no less protective than those provided in this DPA. Upon written request by Data Controller, Data Processor shall make a summary of the data processing terms available to Data Controller. Data Controller may request in writing reasonable additional information with respect to Sub-Processor's ability to perform the relevant Processing activities in accordance with this DPA.
8.3 APPROVED SUB-PROCESSORS. As of the Effective Date, Data Processor engages, as applicable, the following parties as Sub-Processors: 4Mation Technologies India Private Limited, Plat4mation GmbH, Plat4mation ALPS GmbH, Plat4mation BVBA, Plat4mation LLC. Data Processor will notify Data Controller of changes regarding such Sub-Processors through Data Processor's customer support portal (or other mechanism used to notify its general customer base). Each Sub-Processor shall comply with the obligations of the Agreement in the Processing of the Personal Data.
8.4 LIABILITY. Use of a Sub-Processor will not relieve, waive, or diminish any obligation Data Processor has under the Agreement, and Data Processor is liable for the acts and omissions of any Sub-Processor to the same extent as if the acts or omissions were performed by Data Processor.

9. INTERNATIONAL DATA TRANSFERS

9.1 PROCESS OR TRANSFER OF PERSONAL DATA. 4Mation shall not process or transfer any Personal Data outside the European Economic Area (all member states of the European Union, Norway, Iceland, Liechtenstein and , for purposes of this Data Processing Agreement, Switzerland) without the prior written consent of Customer,
9.2 STANDARD CONTRACTUAL CLAUSES AND ADEQUACY. Where required under Data Protection Laws, Data Processor or Data Processor's Affiliates shall require Sub-Processors to abide by (a) the Standard Contractual Clauses for Data Processors established in third countries; or (b) another lawful mechanism for the transfer of Personal Data as approved by the European Commission.

10. LIABILITY / INDEMNIFICATION

10.1 4Mation shall be liable for damages incurred by Customer due to 4Mation not meeting its obligations under this DPA and indemnify and hold Customer harmless against any third party, including expressly fines levied by a Supervisory Authority, claims for infringement of any rights of that third party and against any damages sustained by Customer or by such third party as a consequence of any processing of Personal Data undertaken by the 4Mation in deviation of Customer's instructions or in any way in conflict with or contrary to the Data Protections Laws.
10.2 4Mation's liability for damages and obligation to indemnify as referred to under clause 10.1, shall always be limited to the limitations as agreed in the Agreement and in the event no limitation(s) is(are) agreed in the Agreement, to an aggregate maximum amount of [€ 100.000,00 (hundred thousand Euro].

11. GENERAL PROVISIONS

10.1 In the event of any conflict between the terms of this DPA and the terms of the Agreement with respect to the subject matter herein, this DPA shall prevail. Any data processing agreements that may already exist between Parties as well as any earlier version of the Security Policy Framework to which the Parties may have agreed are superseded and replaced by this DPA in their entirety. All capitalized terms not defined in this DPA will have the meaning given to them in the Agreement.
10.2 The recitals and the Appendices form are an integral part of this Data Processing Agreement.
10.3 This Data Processor Agreement is governed by Dutch law.
10.4 Any dispute arising out of or in connection with this Data Processor Agreement will be settled by the competent court in Utrecht, the Netherlands.

Signed and agreed in [twofold] by the Parties at [place] on the last date specified on the signature page[s].

Customer's official name: ……	Plat4mation B.V.
Individual signing: (print name)	Individual signing: (print name)
Signature:	Signature:
Title:	Title:
Signing date:	Signing date:

APPENDIX 1

DETAILS OF PROCESSING

Nature and Purpose of Processing
Data Processor will Process Personal Data as required to provide the Subscription Service in accordance with the Agreement.

Duration of Processing
Data Processor will Process Personal Data for the duration of the Agreement and in accordance with Section 4 (Data Processor) of this DPA.

Data Subjects
Data Controller may submit Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller, and may include Personal Data relating to the following categories of Data Subjects:
• clients and other business contacts;
• employees and contractors;
• subcontractors and agents; and
• consultants and partners.
Categories of Personal Data
Data Controller may submit Personal Data to the Subscription Service, the extent of which is solely determined by Data Controller, and may include the following categories:
• communication data (e.g. telephone, email);
• business and personal contact details; and
• other Personal Data submitted to the Subscription Service.

Processing Operations
The personal data transferred will be subject to the following basic processing activities:
• All activities necessary for the performance of the Agreement.

Appendix 2

Technical and Organizational Measures (TOM's)

This Appendix 2 forms an integral part of the DPA between the 4Mation and Customer.

I. Description of Technical and Organizational Measures taken by 4Mation as described in the Information Security Policy Framework at http://www.plat4mation.com/legal

Appendix 3

Form for notification of Security Breach

Date:
Time:

Company name:
Address:
Postal code:
Registration Chamber of Commerce:

Who noticed the Security Breach
Name:
Function:
E-mail:
Telephone number:

When was the Security Breach noticed?
Date:
Time:

Description of Security Breach that caused the breach in the security of the Personal Data:

Number of person of which Personal Data are involved in the Security Breach?
a. None, non-Personal Data (company data) are involved.
b. Still to be determined.
c. At least (number), but not more than (number).

Description of the group of individuals whose Personal Data are affected by the Security Breach:

When did the Security Breach happen?
a. On (date + time)
b. Between (date + time) and (date + time)
c. Still to be established
d. Responsible Disclosure by a third party

Type of Security Breach:
a. Just read (a non-authorized third party had access to (confidential) data. Data Processor still has the Personal Data still in its possession).
b. Copy(a non-authorized third party was able to copy Personal Data. The Personal Data are also still in the possession of the Data Processor).
c. Change (a non-authorized third party was able to change Personal Data in the systems of Data Processor)
d. Delete or destroy (a non-authorized third party was able to delete or destroy Personal Data from the systems of the Data Processor).
e. Bribery
f. Still to be established

Categorie(s) of Personal Data involved in the Security Breach:
a. None
b. Name, address, place of residence data
c. Telephone numbers
d. E-mail address, Facebook ID's, Twitter ID's etc.
e. Usernames, customer numbers, passwords, or other access codes ,
f. Financial data, bankaccount numbers, credit card numbers
g. BSN-numbers or sofi numbers
h. Gender, date of birth
i. Other data (description of data involved)::

Are the Personal Date made incomprehensible or made inaccessible for unauthorized use by a third party, e.g. through encryption or hashing?
Yes
No
In part (description):

Description of the manner with which the Personal Date are made incomprehensible or made inaccessible for unauthorized use by a third party:

Does the Security Breach affect persons located in other EU-countries?
Yes
No
Not known

If the answer on the previous question is yes, which out EU-countries:

Description of security measures (technical and organizational) that were taken to cure the Security Breach and avoid further Security Breaches?

Contact person for further information on the Security Breach
a. Person who noticed Security Breach;
b. Contact person:
Name:
Function:
E-mail:
Telephone number: