DESIGN LIFECYCLE MANAGEMENT

ORDER DATA PROCESSING AGREEMENT

DPA

April 2019

Version 1.1

5FLOW

IT SOLUTIONS & MANAGEMENT SOFTWARE

ORDER DATA PROCESSING AGREEMENT

made between

5Flow GmbH
Nikolaus-Otto-Str. 18
52428 Jülich
USt-IdNr: DE 280 690 943

(hereinafter referred to as "5Flow")

Customer
address

(hereinafter referred to as "CLIENT")

PREAMBLE

This Order Data Processing Agreement (**DPA**) forms an integral part of the **ASP and Hosting Agreement** (**Main Agreement**) made between the contracting parties and forms an annex to this Agreement.

1. OBJECT OF THE DPA

1.1. If in accordance with the Main Agreement 5Flow receives the Client's personal data and/or collects, processes or uses the Client's personal data for the Client by order of the Client, the terms of this DPA shall apply.

1.2. 5Flow shall process or use personal data by order of and at the instruction of the Client and in accordance with the terms of this DPA.

1.3. Details of the kind, purpose and scope of the required collection and use of personal data and of the kind of data and the group of data subjects arise are as set out in the Main Agreement and **Annex 1** to this DPA.

2. Place of performance

2.1. 5Flow shall provide the contracted-for services in Germany, and any sub5Flows shall provide the contracted-for services at places of performance in the European Union (EU) or in the European Economic Area (EEA) agreed with the Client.

2.2. The Client shall permit the place of performance to be changed within an approved country of performance, if it can be proved that there is an equal level of security there and there are no legal requirements applying to the Client that prohibit such change. The burden of proof for this lies with 5Flow.

2.3. If the place of performance is changed to countries that are members of the EU/EEA and offer a verified level of data protection that satisfies this Agreement, the Client shall be informed in writing accordingly.

2.4. If within a period of four weeks after receipt of notification as set out in subsection 2.3 about a change of place of performance 5Flow is not informed by the Client about grounds that do not

permit a change of place of performance, the Client's agreement to this change of place of performance shall be deemed to have been given.

2.5. If 5Flow wants to provide the contractually due services partly or wholly from a location outside the EU/EEA in a so-called "third country" or plans to change the place of performance to a place there, 5Flow shall obtain the Client's written approval first.

2.6. If performance can be transferred to another country in accordance with the foregoing provisions, this change shall apply analogously to any access to or any viewing of data by 5Flow, e.g. for the purpose of internal inspections or for purposes of development, conduct of tests, administration or maintenance.

2.7. If data processing in accordance with this Agreement and the requirements of the law for the processing of data is permitted to be undertaken abroad outside Germany, 5Flow shall ensure that the requirements and implementation of the law to ensure that an adequate standard of data protection is met in cases of changes of place of performance and cross-border data traffic.

3. 5FLOW'S OBLIGATIONS

5Flow's obligations as follows:

3.1. 5Flow may collect, process or use data only for the purposes of the Client's order and instructions.

3.2. 5Flow shall within its scope of responsibility organise the company internally so that it fulfils the special requirements of data protection. 5Flow shall take technical and organisational measures that comply with the requirements of the data protection law to appropriately secure the Client's data against misuse and loss; 5Flow shall on request verify to the Client and, if necessary, supervisory authorities that these measures have been taken. This verification shall include in particular the implementation of the measures arising from Art. 32 GDPR. The technical and organisational measures shall be subject to technical progress and further development. To this extent 5Flow is permitted to implement alternative, verifiably adequate measures. It shall be ensured here that the contractually agreed standard of protection is not fallen below. Material changes shall be documented.

3.3. 5Flow itself shall for processing keep a record of processing activities as required by Art. 30 Para. 2 GDPR that it has carried out. 5Flow shall at the Client's request make available to the Client the information required for inspection in accordance with Art. 30 GDPR. 5Flow shall also on request make the record available to the supervisory authority.

3.4. 5Flow shall with all the information available to it assist the Client with the data protection impact assessment. If prior consultation with the relevant supervisory authority should be necessary, 5Flow shall also assist the Client in this regard

3.5. 5Flow shall treat as strictly confidential all knowledge of the Client's company secrets and data security measures to which it may become privy during the contractual relationship.

3.6. Dr. Stefan Baum c/o Datenschutz und Compliance GmbH, Humboldtstr. 3, 79539 Lörrach (datenschutz@5flow.eu), has been designated current External Data Protection Officer at 5Flow. The Client shall be informed in writing immediately of any change of data protection officer. 5Flow warrants that the requirements made of the data protection officer and his function will be satisfied as set out in Art. 38 GDPR. If no data protection officer has been designated at 5Flow, 5Flow shall name to the Client a contact person.

3.7. 5Flow shall notify the Client immediately of infringements of the regulations for the protection of the Client's personal data or the provisions of the Agreement committed by 5Flow or persons employed by 5Flow for the purposes of the order. 5Flow shall take the necessary measures to secure the data and to mitigate any possible detrimental consequences for data subjects and shall immediately consult with the Client in this regard. 5Flow shall as required by Art. 33, 34 GDPR assist the Client in fulfilling the obligations of information to the currently relevant supervisory authority and/or the persons affected by infringement of personal data protection.

3.8. If a person affected applies direct to 5Flow for rectification or deletion of his data, 5Flow shall immediately pass on such application to the Client.

3.9. Provided data carriers and all copies or reproductions of such shall remain the property of the Client. 5Flow shall keep these safe so that they are not accessible to third parties. 5Flow shall inform the Client at any time if his data and documents are affected.

3.10. If the Client is at any time required under data protection legislation to collect, process or use information from a data subject for such data subject, 5Flow shall assist the Client to provide such information, provided that Client has requested 5Flow to do so in writing.

3.11. 5Flow shall inform the Client immediately of any inspections and measures by supervisory authorities or if a supervisory authority is investigating 5Flow.

3.12. 5Flow shall notify the Client immediately, if in 5Flow's opinion an instruction given by the Client breaches legal regulations. 5Flow may set aside implementation of the instructions concerned until it is confirmed or amended by the Client.

3.13. If the Client's data at 5Flow are under threat of distraint or confiscation or may be subject to an insolvency or settlement procedure or to events at or measures taken by third parties, 5Flow shall notify the Client of the fact immediately. 5Flow shall inform all persons responsible in this regard that right of disposition and ownership of the data lies solely with the Client as controller as defined by the GDPR.

3.14. 5Flow shall not use the provided data for any purposes other than performance of the Agreement and shall not use any other means for processing them that have not first been approved by the Client.

3.15. If 5Flow is required by the law of the Union or member states also to process the data in another way, 5Flow shall before processing notify the Client of such legal requirement. The notification shall not be made, if relevant national law prohibits such notification because of an important public interest.

3.16. Fulfilment of the foregoing obligations must be monitored, documented and on request verified to the Client by 5Flow in an appropriate manner.

3.17. All assistive services shall be requested in writing. The Client shall reimburse 5Flow the costs incurred through this assistance.

4. CLIENT'S RIGHTS AND OBLIGATIONS

4.1. The Client alone shall be responsible for assessment of the reliability of the data processing and of respecting the rights of data subjects. The Client shall within his scope of responsibility ensure that the legally necessary conditions are created (e.g. by obtaining declarations of approval for processing the data) in order that 5Flow can provide the agreed services without breaking the law.

4.2. The Client shall notify 5Flow immediately and fully if during the inspection he discovers errors or irregularities in respect of the requirements of data protection law.

4.3. The Client shall under data protection law be responsible for processes and procedures approved by the Client for the automatic processing of personal data and in addition to 5Flow's obligation to do so also has the duty of keeping a record of processing activities.

4.4. The Client shall also be responsible in accordance with Art. 33, 34 GDPR for providing information to the supervisory authority or persons affected by breaches of the personal data protection regulation.

4.5. The Client shall contractually or by instruction specify measures for return of the provided data carriers and/or for deletion of the stored data after termination of the order.

4.6. The Client shall treat as confidential all knowledge of 5Flow's company secrets and data security measures to which the Client shall become privy during the contractual relationship.

4.7. The Client shall ensure that he for his part adheres to the requirements arising from Art. 32 GDPR in respect of security of processing. This applies in particular to remote accessing by 5Flow of the Client's data sets.

4.8. If the Client makes individual instructions that go beyond the contractually agreed scope of services, the costs incurred thereby shall be paid by the Client. If the agreed scope of services is exceeded, a prior separate written agreement must be reached for this.

5. Client's right to inspect

5.1. The Client has decided to engage 5Flow because 5Flow offers sufficient warranties that it will take technical and organisational measures to ensure that processing is carried out in accordance with the requirements of the GDPR and warrants that it will respect the rights of data subjects. It shall document the result of its decision.
For this it may, for example,

- take into consideration data-protection-specific certifications,
- obtain written self-disclosure from 5Flow or

- after giving due notice ascertain for itself in person or have a third party that is not in competition with 5Flow ascertain during normal business hours without disrupting business procedure that the agreed terms and conditions are being adhered to.

5.2. If 5Flow has or persons engaged to help perform an order have committed a breach of the regulations for protection of the Client's personal data or of the contractual provisions, an inspection to this effect may be conducted with or without due notice. Disruption of the business routine at 5Flow must then as far as possible be avoided.

5.3. Order checking by means of regular inspections by the Client with regard to contract performance or fulfilment, particularly adherence to and, if necessary, necessary adaptation of provisions and measures for performance of the order, shall be assisted by 5Flow. In particular 5Flow shall furnish to the Client on written request and within an appropriate period of time all the information necessary to conduct an inspection.

5.4. The Client shall notify 5Flow immediately and fully if during the inspection it identifies errors or irregularities in respect of the requirements of data protection law.

6. Subcontractors

6.1. The Client agrees that 5Flow may engage 5Flow's affiliated companies to help perform its contractually agreed services. However, each subcontractor (affiliated company) shall before being engaged be notified to the Client in writing so that the Client may, if there are compelling grounds to do so, refuse the engagement. If the Client refuses his agreement on any other than compelling grounds, 5Flow may terminate the Agreement at the time at which the subcontractor is scheduled to start work.

6.2. At the time at which this Agreement is made the contractually agreed services or part-services specified below shall be performed with the help of a sub5Flow, namely

Name and address of subcontractor	Description of part-services
PlusServer GmbH, Hohenzollernring 72, 50672 Köln	Hosting services

6.3. 5Flow shall take care to engage only subcontractors that are especially suitable for fulfilment of the technical and organisational measures agreed between the Client and 5Flow.

6.4. If under this Agreement 5Flow is authorised to engage the services of a subcontractor in order to carry out specific processing activities on the Client's behalf, such subcontractor shall be bound by contract to fulfil the same obligations as those provided between the Client and 5Flow in this Agreement, particularly in respect of the requirements for confidentiality, data protection and data security between the parties to this Agreement and the Client's rights to inspect and audit described in this DPA. Here sufficient warranties shall also be given that the appropriate technical and organisational measures will be implemented in such a way that processing is done in accordance with the requirements of the GDPR.

6.5. The Client may by written request ask 5Flow to provide information about the subcontractor's data-protection-related obligations, if necessary, also by inspection of the relevant Agreement documents.

6.6. A subcontractor relationship requiring approval shall not have been entered into if 5Flow engages third parties to perform a service subsidiary to the main service, such as for personnel, postal and despatching services. However, 5Flow shall to ensure the protection and security of the Client's data, including externally provided subsidiary services, make appropriate and legally compliant contractual agreements and take inspection measures. The subsidiary services shall be stated in detail beforehand.

6.7. If the subcontractor does not fulfil his data protection obligations, 5Flow shall be liable to the Client for fulfilment of such subcontractor's obligations.

7. Liability

The terms of liability agreed between the parties in the Main Agreement shall also apply to order processing.

8. Other requirements

8.1. 5Flow shall pay all the costs incurred by it in connection with the fulfilment of its obligations under this Work Agreement.

8.2. This DPA shall begin to run at the time at which the Main Agreement enters into force and effect and shall continue to run until the time at which the Main Agreement ends. If after the end of the Main Agreement processing of personal data by 5Flow is necessary or required by law for processing and performance of the Main Agreement, for example, in respect of the surrender of personal data, this Work Agreement shall remain in force and effect until processing and performance are completed.

3.1. No rights of retention shall apply in respect of the processed data and the associated documents and data carriers.

3.2. 5Flow's obligations under requirements of the law or authority or court orders shall not be affected by this Work Agreement.

3.3. This DPA represents in due consideration of the Main Agreement all the terms and conditions in respect of the object of contract. Changes or additions to or cancellation of this DPA shall be made in writing. This term shall also apply to a term under which this writing requirement clause is waived.

5Flow GmbH	**Client**
Robert Mertens Name	_____ Name
Company Management Function	_____ Function
Jülich, Place, date	_____ Place, date
_____ Signature	_____ Signature

Annex 1 – Details of data processing

1. SCOPE AND PURPOSE OF DATA PROCESSING

5Flow shall within the scope of its technical and operational possibilities make available to the Client on the basis of the ASP and hosting agreement the - Webfrontend for control of the Design Lifecycle Workflow (product name WAVE hereinafter referred to as "WAVE").

In this connection 5Flow shall as far as is necessary collect, process or use the Client's and other legitimate WAVE users' personal data in order to provide WAVE for the purposes of performance of the Main Agreement and enable its functionalities.

2. KIND OF PERSONAL DATA AND GROUP OF DATA SUBJECTS

2.1 Users' data through 5Flow (administrator, developer and support staff):

User's name, email address, telephone number,

2.2 *Data of Client's employees, Client's members' and subsidiary companies:*

Name, email, address, telephone, function in the company, use data such as login and all process data traceable in the portal history that are stored in connection with a user name.

2.3 *Data of employees of Client's collaboration partners (suppliers and other persons involved in the process):*

Name, email, address, telephone, function in the company, use data such as login and all process data traceable in the portal history that are stored in connection with a user name.

Kind of data	Category of data subjects	Kind and purpose of data processing
The following data will be processed: - personal master data - user data - communication data - protocol data	Persons affected by the processing: - employees - contact persons - software users	The Contractor shall provide for the Client the following services and activities during which a possibility of access to personal data cannot be excluded: - configuration and provision of system - inspection/maintenance and continuous monitoring of the

Annex 2

Contractor's technical and organisational measures

Measures in accordance with Art. 32 Para. 1 GDPR and Annex

Integrity (Art. 32 Para. 1 Point b GDPR)

Disclosure check
No unauthorised reading, copying, changing or removal during electronic transmission or transport: amongst other things there will be encryption of data during transport, a Virtual Private Network (VPN) will be used for communication.
Data will not be disclosed to third parties. The data will be merely duplicated for data security purposes within the encapsulated system.

Input check
No contract data processing as defined by Art. 28 GDPR shall be carried out without the Client's instruction. Data shall be entered by the Client himself or in individual cases by a separate order of the 5Flow administrator. A user identification check will be made. (Login process) Specification whether and by whom personal data will be entered or changed in or removed from data processing systems: amongst other things logging will take place for access

Availability and load capacity (Art. 32 Para. 1 Point b GDPR)

Data shall be appropriately protected by means of technical and organisational measures against accidental or deliberate destruction or loss and may in case of emergency be reinstated at sufficient speed: amongst other things by means of data security, uninterrupted power supply (UPS), virus protection and firewall

Data shall be stored and hosted on a separate virtual server cluster in an encapsulated VMWare system secured with a separate firewall at the subcontractor PlusServer GmbH, Hohenzollernring 72, 50672 Köln (im Folgenden PlusServer).

Availability checks shall be conducted solely by PlusServer

The following availability check measures will be taken at PlusServer:

- data security concept
- backup procedures
- mirroring of hard disks, e.g. RAID process
- uninterrupted power supply (UPS)
- firewall

Confidentiality (Art. 32 Para. 1 Point b GDPR)

Data access check
Data shall be located solely on the PlusServer company's servers; amongst others the following security measures have been agreed here:

- PlusServer computer centres will be spatially distributed and will not be identifiable as such from outside.
- Road information will be disclosed only on request.
- Entrances and server rooms will be videomonitored, Recording 24 hours / 3 weeks
- An alarm system with movement detectors will monitor the entire building complex.
- Access will be permitted only to authorised contracting parties with advance appointment who can identify themselves on site. Authorised representatives will require a written confirmation from the contracting party.
- Access to the server rooms will be possible only in the company of an employee.

Physical access check
Access check by means of digital locking system with PIN, access or fingerprint clearance on three access levels (reception/work room/server room).
Doors are self-closing, and access is also possible for authorised persons only within the time window/working hours.
Access will be continuously recorded.

Data access check
Differentiated authorisations.
An authorisation concept is in place that is implemented by 5Flow and specifies rights of physical access for each user accordingly. No unauthorised reading, copying, changing or removal within the system: amongst other things needs-based access rights are granted according to activity areas with the least rights in each case; access will be recorded;

Only 5Flow's IT staff will have access to the Client's actual personal data. Only these staff members will have administrator rights and have declared that they agree to abide by all the requirements of data protection law.

Separation check
All data will be collected and processed only for the one single order under the contract. No personal data will be stored at 5Flow. Separate processing of data that have been collected for different purposes: amongst other things by means of processing-specific multi-client software.

The separation check will be conducted by means of the following measures:

- separation of productive and test systems will be ensured
- no real user data will exist in the test system
- separate data bases/in separate server area
- when transmitting personal data on the Internet, the SSL encryption procedure will be applied.

Pseudonymisation (Art. 32 Para. 1 Point a GDPR; Art. 25 Para. 1 GDPR)
If necessary and appropriate, data shall be pseudonymised order- and service-specifically in a technically suitable manner. Users who have been declared in the system as non-active users shall be pseudonymised in the following step. This will make it difficult to trace user data and will not interfere with the actual business process.
Pseudonyms are cryptic and will not be stored n relation to the original user data.

Data protection management

We attach exceptional importance to the protection of personal data. For this reason continuous improvement of data protection is part of our quality management in the company. All processes relating to personal data are in accordance with the PDCA principle continuously audited, adapted, documented and installed in our management system under strict control.

Incident response management

Continuous monitoring enables any form of fault in the whole IT process to be identified as fast as possible. At the forefront here are preventive measures such as continuous monitoring of requests to the processing system.

Regular code scanning and penetration tests by external providers assist continuous improvement and prevent possible faults.

Robust incident management and suitable forensic measures are documented in our quality management system.