DATA PROCESSING ADDENDUM

Last modified: 29.10.2026.

1. Introduction

1.1. In order to easily track the changes of the present Data Processing Addendum (hereinafter as: **"DPA"** or **"Addendum"**), we summarized the changes in the below table including the effective dates and a short description of what has been changed:

Version	Date	Change
v6	29.10.2026	Alignment of security reviews with ISO/IEC 27001:2022 and clarification of Trust Center disclosures and access to audit results. (section 10.2 and section 12.8.)
v5	30.01.2026 - 28.10. 2026.	Clarification of responsibilities (new section 7.5.)
v4	11.10.2023 - 29.01.2026	General stylistic and structural changes to improve consistency and clarity
v3	15.12.2022 – 10.10.2023.	Amendment of the DPA with further appendixes regarding EU and international data transfers
v2	18.07.2022.- 14.12.2022	Change of premise (Section 10.4.)
v1	23.12.2019.-17.07.2022	Initial version

1.2. Present DPA forms an inseparable part of the Terms of Use (hereinafter as: **"Agreement"**) entered into force by META-INF and the Authorized User of the META-INF Apps and contains the provisions on the processing of personal data pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter: **"GDPR"**) between the Authorized User as Controller and META-INF as Processor and on international data transfers and data transfers within the European Economic Area.

1.3. By accepting the terms of the Agreement, the provisions of present DPA becomes also binding without any further action and without it being signed.

1.4. Unless otherwise provided herein the terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified below, the terms of the Terms of Use shall remain in full force and effect.

1.5. In consideration of the mutual obligations set out herein, the Parties hereby agree that the DPA set out below shall be added as an addendum to the Agreement with all its appendixes.

2. Definitions

Authorized Representative of the Customer – The technical contact given at the time of the purchase of the Atlassian License and the official representative of the Customer who has signatory right shall be deemed as authorized representative. Any changes in the person of the Authorized Representative of the Customer shall be sent to the following e-mail address: privacy@meta-inf.hu

Authorized Representative of the Processor – The contact person of the Processor to whom the Customer shall send any instructions regarding the Processing of Customer Data and who are entitled to receive such instructions on behalf of the Processor and have the authority to take the necessary measures. The list Authorized Representatives of the Processor is enclosed as Appendix no. 1 (https://www.metainf.hu/en/dpa-appendix-1/)

Customer – Who purchased a cloud deployment META-INF App through Atlassian Marketplace or from any other legitimate sources;

Controller – The Customer; otherwise shall have the meaning given in the GDPR

Customer Data – any personal data for which the Customer is the Controller, and which shall be forwarded for processing to Processor. also means any personal data provided by (or on behalf of) the Customer to META-INF in connection with the Services including the Personal Data of End Users

DPA – the present Data Processing Addendum

Data subject – shall have the meaning given in the GDPR

EEA – means the European Economic Area*;*

End Users – means an individual the Customer gives permission or invite to use the Services. For the avoidance of doubt: (a) individuals invited by the Customer's End Users, (b) individuals under managed accounts, and (c) individuals interacting with the Services as the Customer's client are also considered End Users.

GDPR – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Parties – Controller and Processor jointly.

Personal Data – shall have the meaning given in the GDPR

Processor – META-INF Szolgáltató Korlátolt Felelősségű Társaság (seat: Taksony utca 6. fszt. 1., Budapest, 1192, Hungary, company registration number: 01-09-170431) who is the processor of the Customer Data; otherwise shall have the meanings given in the GDPR

Processing or Data Processing – shall have the meanings given in the GDPR

Subcontractors – Any third party who are in contractual relationship with the Processor and who may also conduct processing activity in connection with the Customer Data.

Sub-processors – means any processor engaged by the Processor to assist in fulfilling its obligations with respect to providing the Services pursuant to the Agreement or this DPA where such entity processes Customer and End User Data. As a general rule Sub-processors are the same as the Subcontractors but may also include META-INF's affiliates or other third parties. The list of Sub-processors whose engagement is accepted by the Controller automatically by accepting the terms of this DPA is enclosed as Appendix no. 1A to this DPA (https://www.meta-inf.hu/en/dpa-appendix-1a/)

Security Incident – means any confirmed unauthorized or unlawful breach of security that leads to the accidental, unauthorized, or unlawful destruction, loss, alteration, disclosure of or access to Customer Data

processed by the Processor and/or its Subcontractors in connection with the provision of the Services. "Security Incident" does not include unsuccessful attempts or activities that do not compromise the security of personal data, including unsuccessful login attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

Services – means providing license and access to the META-INF Apps pursuant to the Agreement

3. Scope of the DPA

3.1. Within the framework of performance of the Agreement (**https://www.meta-inf.hu/en/terms-of-use**) it is necessary for META-INF as Processor to deal with personal data for which the Customer is the Controller. Present DPA contains the provisions, in particular the data protection rights and obligations of the Parties, concerning the Processor's Processing of Customer Data for performance under the Agreement.

3.2. Notwithstanding the provisions of Section 3.1. the relationship between the Parties may be as follows:

a) Where the Customer is Controller of Customer Data covered by this DPA, META-INF shall be a Processor Processing Personal Data on behalf of the Customer and this DPA (and its appendixes) shall apply accordingly;
b) Where Customer is Processor of Customer Data covered by this DPA, then META-INF shall be a Subprocessor of the Personal Data and this DPA (and its appendixes) shall apply accordingly;

c) Where and to the extent META-INF Processes Personal Data as a Controller, META-INF will Process such Personal Data in compliance with its privacy policy (hereinafter as: **"Privacy Policy"**) (**https://www.meta-inf.hu/en/privacy-policy/**) and the applicable data protection laws and this DPA to the extent applicable

3.3. The Processor declares that as a general rule it shall process the personal data exclusively within the EEA. Data is Processed outside the EEA under Subcontracting / Sub-processing relations to which the provisions of Section 5. shall prevail

3.4. If the Processor Processes Customer Data in a third country (i.e., outside the EEA), it shall require the Controller's prior written or electronically documented consent and shall only occur to the extent that the special requirements of the GDPR are met. If the Commission decides that a third country offers an adequate level of data protection, no further authorization is needed to transfer the Customer Data. The Processor informs the Controller that the Customer Data may be Processed outside the EU at a third country (as of the effective day of this DPA, the Customer Data may be Processed in the territory of United States of America in compliance with the regulations of the relevant SCCs), therefore no written authorization is required based on Article 45 of GDPR.

4. Nature, duration, scope, and purpose of the Processing

4.1. The Processor shall Process Customer Data only on behalf of the Controller if necessary to perform its obligations under the Agreement and upon documented lawful instructions of the Controller (as set forth in the Agreement or this DPA) (hereinafter as: **"Permitted Purpose"**). By using the respective cloud deployment product, the Processor issues the instructions for Data Processing.

4.2. The Processor shall exclusively Process the Customer Data as described in the Privacy Policy. The Processing of Customer Data by the Processor relates exclusively to the categories of Data Subjects subsequently described in the Privacy Policy.

4.3. The Processor is prohibited from any Processing of Customer Data that deviates from or extends beyond the Permitted Purpose, in particular use of the Customer Data for its own purposes and may not sell or otherwise utilize them, an exception for the deviation of Permitted Purpose may occur where it is required by law(s) that are not incompatible with any applicable data protection law. The Controller is also obliged

not to provide the Processor any personal data not stipulated in the Privacy Policy until the Privacy Policy has been updated accordingly.

4.4. The Data processed by the Processor are described in Appendix no. 2 of the present Agreement (https://meta-inf.hu//en/dpa-appendix-2)

4.5. The duration of processing Customer Data shall be in line with the duration of the Agreement taking into account the provisions of Section 14 of present DPA.

4.6. The Customer agrees that in the course of its own Processing of Customer Data and any processing instructions it issues to META-INF (i) it will comply with its obligations under applicable data protection laws; and (ii) it has provided notice and obtained (or will obtain) all consents and rights necessary under applicable data protection laws for the Processor to Process Personal Data (including but not limited to any special categories of data) and pursuant to the Agreement (including this DPA).

4.7. The Parties shall be able to demonstrate compliance with the GDPR and present DPA.

5. Data transfers

5.1. With respect to the provisions of Section 3.4. the Processor declares that it uses appropriate measures for any data transfers made under and in compliance with the Agreement (including this DPA).

5.2. For data transfers within the EEA the provisions of the GDPR and present DPA are applicable.

5.3 For international data transfers the provisions of the DPA and present DPA are also applicable. The Processor informs the Controller that the Personal Data may be stored outside the EEA, which the Controllers agrees by accepting the present DPA. The Processor undertakes the obligation that in such case, prior to the data transfer it (i) informs the Controller about the data transfer to a third country, and through whom it will be carried out (ii) concludes the agreements in accordance with the applicable legislation, which are necessary for the data transfer to take place, if required under the GDPR.

5.4. In case the Alternative Mechanism does not cover all territories or the full scope of Personal Data Processed under present DPA the Processor undertakes to amend present DPA to comply with the GDPR and any other applicable data protection law.

6. Authority of the Controller

6.1. The Processor shall exclusively Process the Customer Data in accordance with the provisions contained in this DPA and other lawful instructions of the Controller. The Processor is entitled to refuse the fulfilment of any instructions of the Controller if it would breach the provisions of the GDPR or any other applicable data protection law or the provisions of this DPA.

6.2. The Controller shall issue all instructions and orders in a documented electronic format. For this purpose, the Parties establish that communication by e-mail shall suffice.

6.3. The Controller is obliged to confidentially treat all knowledge of the Processor's business secrets and data security measures acquired within the framework of the contractual relationship. This obligation shall remain in force even after the termination of this DPA.

6.4. As a general rule, instructions are to be issued by the Controller's Authorized Representative. The Processor informs the Controller that it only accepts instructions from the Authorized Representative. The Controller shall notify the Processor of any changes in those authorized to act or their substitutes, naming a representative as soon as possible via privacy@meta-inf.hu

6.5. If the Processor has reasonable belief that an instruction from the Controller infringes this Agreement or the applicable data protection law, it must notify the Controller immediately. After timely prior notification to the Controller of at least a 14-day period, the Processor is to suspend implementation of the instruction

pending confirmation or change of instruction by the Controller. If the Controller confirms the instructions with a brief justification in writing, the Processor is obliged to follow them. In this case, the Parties agree that the Controller alone shall be liable for the lawfulness of the processing.

7. Rights and duties of the Controller

7.1. Externally, in particular to third parties and Data Subjects, the Controller is solely liable for the assessment of the lawfulness of the Personal Data Processing and for the protection of the rights of Data Subjects. Nevertheless, as far as legally permissible, the Processor is obliged to forward all requests by Data Subjects to the Controller, as far as these are recognizably directed to the Controller. The Processor shall assist the Controller appropriately in answering requests from Data Subjects (such as rectification, erasure, and restriction of processing) and is entitled to charge reasonable compensation if the requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character. In such a case the Processor may charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested in line with Subsection 5 of Section 12 of GDPR.

7.2. The Controller is the owner of the Customer Data and, in the relationship of the Parties to each other, holder of any rights to the Customer Data.

7.3. The Controller shall be responsible for providing the Customer Data to the Processor in right time for contractual performance under the Agreement. Further, the Controller shall be liable for the quality and lawfulness of collection of the Customer Data. The Controller must notify the Processor immediately and fully if it finds errors or irregularities regarding data protection regulations or its instructions when examining the results contracted.

7.4. In the event that a third party or Data Subject brings a claim directly against the Processor for violations of rights and/or any related claims, the Controller undertakes to indemnify the Processor for all damages, costs/fees, including legal or other expenses or losses arising from the claim, to the extent that the Processor has notified the Controller of the assertion of the claim and has given it the opportunity to cooperate with the Processor in defending against the claim.

7.5. The liability in the internal relationship between the Controller and the Processor is based on the proportionate fault within the meaning of Article 82 GDPR.

8. Rights and duties of the Processor

8.1. The Processor is obliged to process personal data exclusively within the framework of the Agreement made pursuant to the instruction of the Controller. This shall not apply if the Processor is obliged to perform other processing under EU law or any Member State law to which the Processor is subject to (e.g., investigations by state authorities or law enforcement agencies). In this case, the Processor shall notify the Controller of these legal requirements prior to Processing, unless the law in question prohibits such notification due to a significant public interest.

8.2. The Processor shall not use the Customer Data provided by the Controller for processing for any other purpose as described in this DPA, in particular for its own purposes. The Processor shall not make copies or duplicates of the Customer Data without the Controller's prior written consent. Even with the prior written Consent of the Controller the Processor is not entitled to make copies or duplicates of the Customer Data except for data backup and cluster technology purposes.

8.3. If the Processing involves Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter as: **"Sensitive Data"**), the Processor shall apply specific restrictions and/or additional safeguards. For the use of META-INF Apps the processing of sensitive data is not necessary, therefor primarily Customer is responsible not to enter such data into META-

INF Apps. If preceding is not possible, then still primarily Customer as data controller is responsible to be appropriately authorized to use sensitive data within the META-INF Apps.

8.4. The Processor shall ensure that any person that it authorizes to Process Customer Data (including employees, agents, and Sub-processors, hereinafter together as: **"Authorized Person"**) shall be subject to a duty of confidentiality (whether a contractual duty or a statutory duty) and shall not permit any person to Process Customer Data who is not under such a duty of confidentiality.

8.5. The Processor shall not hand over Customer Data to third parties or other recipients without the Controller's prior written consent. Exceptions to this include data transfers to Subcontractors whose assignment the Controller has accepted.

8.6. The Processor shall only provide third parties or authorities with information about personal Customer Data from this contractual relationship to the extent legally permissible, after prior written or electronically documented instructions or approval by the Controller.

8.7. If the Controller is obliged to provide information about the Customer Data or the processing thereof to a governmental body, Data Subject or another person, the Processor is obliged to assist the Controller in the provision of such information, at first request, in particular by immediately providing all information and documents concerning the contractual processing of the Customer Data, including the technical/organizational measures taken by the Processor, the technical procedure in using the Customer Data, the locations where the Customer Data is used and the employees involved in the Processing.

8.8. The Parties further agree that in this case if there is a request from a third party regarding a Customer Data processed on behalf of the Controller, the Processor will forward such request to the Controller, to the email address of the technical contact. Any communication sent to this e-mail shall be deemed as official communication. The Controller is responsible to make the necessary actions regarding the request. Failing to fulfil this obligation in time or accordingly with the provisions of the GDPR or any applicable laws is the sole liability of the Controller, and it must exonerate the Processor for any liability.

8.9. The Processor shall not respond to any communication it receives pursuant to Section 8.8. above directly without the Controller's prior written authorization, unless legally compelled to do so, and instead, after being notified by the Processor, the Controller shall respond. If the Processor is legally required to respond to such a request, the Processor will promptly notify the Controller and provide it with a copy of the request unless legally prohibited from doing so.

8.10. If a law enforcement agency or other similar authority sends the Processor a demand for Customer Data (e.g., a subpoena or court order erc.), the Processor will attempt to redirect the law enforcement agency to request that data directly from the Controller. As part of this effort, the Processor may provide the Controller's contact information to the law enforcement agency. If compelled to disclose the Controller Personal Data to a law enforcement agency, then the Processor will give the Controller reasonable notice of the demand to allow the Controller to seek a protective order or other appropriate remedy to the extent the Processor is legally permitted to do so.

8.11. The Processor undertakes to:

a) fulfil the rights of the data subjects,
b) fulfil the obligation under GDPR,
c) prepare directories of processing activities,

8.12. The Processor undertakes to cooperate to the extent necessary and adequately assisting the Controller as much as possible. The respective information required for this shall be forwarded to the Controller upon its written request.

8.13. The Processor shall be obliged to rectify, erase, or restrict the Processing of Personal Data resulting from this contractual relationship if the Controller so requests by means of a written or electronically documented

instruction and this does not conflict with the Processor's legitimate interests, in particular the observance of statutory provisions.

8.14. The Processor informs the Controller that some of its META-INF Apps Process e-mail messages, therefore if the Costumer Data intended to be deleted could be found in the body of the e-mail message, the Processor would only be able to fulfil the request of the Controller if the Controller presents the exact e-mail message, in which the Customer Data can be found. The Processor fulfils its obligation to erase it by deleting the entire e-mail.

8.15. Both the Controller and the Processor shall agree on making any changes in the Processing subject matter only by their mutual agreement. The Parties further agree that the Processor is entitled to make changes in the Processing procedure by its sole discretion, but such change shall not be more disadvantageous than the former procedure. These changes (change in processing subject or in Processing procedure) shall be recorded in writing or in a documented electronic format.

8.16. The Processor is entitled to process data outside the office premises (e.g., with the Processor's employees working from home) according to the applicable strict confidentiality and security obligations.

9. Confidentiality obligation and observance of secrecy rules

9.1. The Processor confirms that it is familiar with the relevant GDPR data protection regulations, in particular with regards to Processing.

9.2. The Processor undertakes to maintain confidentiality in the orderly processing of the Controller's Personal Data and Customer Data. This shall continue after the termination of the Agreement.

9.3. The Processor warrants that it shall familiarize those employed (or sub-contracted by the Processor) in carrying out the data processing, prior to commencing the activity, with the data protection provisions relevant to them. For the term of their employment and after termination of employment, these employees must undertake to maintain the appropriate confidentiality.

10. Technical and organizational measures

10.1. The Processor shall take all technical and organizational measures required to maintain the necessary Processing levels during the contractual period to ensure that the level of protection of the rights and freedoms of individuals affected by the Processing is appropriate for the specific Processing agreed. The protection objectives, such as confidentiality, integrity and availability of systems and services, as well as resilience in terms of the nature, scope, circumstances, and purpose of the processing shall be taken into account in order to minimize risk during the contract period. The exact security, technical and organizational measures taken by the Processor, which shall also be considered as a security standard (hereinafter as: **"Security Standards"**) are listed in Appendix no. 3. of this DPA (https://www.metainf.hu/en/dpa-appendix-3/).

10.2. The Processor shall, at planned intervals and as part of the audit and review cycle under its information security management system certified to ISO/IEC 27001:2022, test, assess and evaluate the effectiveness of the technical and organizational measures implemented to ensure the security of the Processing of Customer Data.

Information concerning the Processor's then-current certifications, published controls, and relevant information security and compliance documentation shall be maintained and made available through the Processor's Trust Center at https://trust.meta-inf.hu. Security-sensitive or confidential materials may be made available subject to appropriate access controls and confidentiality obligations.

10.3. The Controller shall notify the Processor if the measures taken by the Processor do not meet the Controller's requirements.

10.4. During the contractual relationship, the Processor is entitled to adapt measures to technical and organizational developments, provided that these do not fall below the standards agreed upon.

11. Notification obligations of the Processor in case of processing disruptions and Security Incidents

11.1. With regards to Customer Data Processing, the Processor is obliged to notify the Controller of any disruptions or breaches of data protection regulations or the provisions hereof by the Processor (or those with access to Customer Data employed by the latter).

11.2. The Processor is further obliged to notify the Controller immediately of any Security Incident or major irregularities in the Processing of the Controller's Personal Data or the Customer Data, in particular if there is evidence - for whatever reason - that a third party may have obtained unlawful knowledge of the Customer Data or if the integrity or confidentiality of the Controller's data is endangered in any other way.

11.3. Notifications pursuant to Articles 33 (Notification of a personal data breach to the supervisory authority) and 34 (Communication of a personal data breach to the data subject) of GDPR may only be made by the Processor to the Controller upon prior written or electronically documented instructions.

11.4. Upon becoming aware of a Security Incident, the Processor shall inform the Controller without undue delay and shall provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer to allow the Controller to fulfil its data breach reporting obligations under the applicable data protection laws. The Controller shall further take reasonable steps to contain, investigate, and mitigate the effects of the Security Incident. Atlassian's notification of or response to a Security Incident in accordance with this Section shall not be construed as an acknowledgment by the Processor of any fault or liability with respect to the Security Incident.

11.5. The notification sent by the Processor pursuant to Section 11.4. above shall contain information especially on the following:

a) a description of the nature of the Security Incident (including, where possible, the categories and approximate number of data subjects and data records concerned);
b) the details of a contact point where more information concerning the Security Incident can be obtained;
c) its likely consequences and the measures taken or proposed to be taken to address the Security Incident, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

12. Control rights of the Controller

12.1. Before beginning the Processing and regularly thereupon, the Controller is entitled to verify, in an appropriate way, the compliance of the technical and organizational measures taken by the Processor and the obligations set out herein, as well as the compliance with the relevant legal data protection provisions. If the Controller ascertains errors or irregularities in this or in any other examination of the agreed outcomes, the Processor shall be notified immediately thereof.

12.2. To carry out the checks, the Controller is entitled to enter the Processor's business premises where the Customer Data is processed (provided that it is fully at the disposal of the Processor) during normal business hours (according to the Marketplace Listing of the product at marketplace.atlassian.com) at its own expense, without disrupting operations, and strictly maintaining the secrecy of the Processor's business- and trade secrets.

12.3. The Controller shall notify the Processor in due time (usually at least two weeks in advance) of all circumstances related to carrying out the inspection. As a rule, the Controller may carry out one inspection

per calendar year. Notwithstanding this, the Controller's right remains to carry out further checks in the event of special occurrences.

12.4. The Processor shall grant the Controller all rights of information and inspection required by the Processor to carry out the inspection. In particular, the Processor undertakes to grant the Controller access to the data processing equipment, files, and other documents to enable the monitoring and verification of the relevant data processing equipment, files and other documentation related to Customer Data Processing as stipulated below, through its employee:

a) The Controller is granted the possibilities of investigation only at the premise located at HUNGARY, 1117 Budapest, Irínyi József utca 4-20;
b) The Controller will provide a dedicated employee, who has full, unlimited access to the Customer Data;
c) The dedicated employee may retrieve all data regarding the respective Customer Data in case of the explicit inquiry of the Controller;

The Processor further informs the Controller, that it – indirectly - grants all access and fulfils its obligation through its employee, which means the Processor will not grant direct access to any files, documents etc. to the Controller. All inspection must be made through the Processor's employee.

12.5. The Processor shall provide the Controller with all information required for the inspection. The Controller hereby takes due consideration of the Processor's operating procedures and legitimate confidentiality interests.

12.6. The Processor shall receive a reasonable lump-sum allowance from the Controller for each of its inspections within the scope of these checks.

12.7. If the Controller commissions a third party to carry out the inspection, the Controller must oblige the third party, in writing, as the Controller is also obliged to the Processor. In addition, the Controller must oblige the third party to confidentiality and compliance with rules to protect confidential information, unless the third party is already subject to a professional confidentiality obligation. At the Processor's request, the Controller must immediately provide it with the confidentiality agreements with the third party. The Controller undertakes not to entrust the inspection to any competitor of the Processor.

12.8. Upon written request, the Processor shall provide the Controller with the Processor's then-current certifications and, to the extent relevant to the Processing of Customer Data, a summary of the results of applicable internal or external audits, including any material findings and the status of related corrective actions.

The Processor may provide such information in executive-summary or reasonably redacted form where necessary to protect confidential information, trade secrets, the security of its systems, or third-party rights, provided that the information supplied is sufficient to demonstrate compliance with this DPA.

The Processor shall fulfil one such request per calendar year free of charge. This annual limitation shall not apply in the event of a Security Incident, a special occurrence referred to in Section 12.3, or where additional information is required by applicable data protection law or a competent supervisory authority. Additional requests not falling within the preceding sentence may be subject to the Processor's reasonable costs. The provision of information under this Section 12.8 shall not constitute an inspection for the purposes of Section 12.6.

13. Subcontracting / Sub-processing relationships

13.1. The Controller agrees that the Processor may engage Sub-processors to process Customer Data on the Controller's behalf.

13.2. The Processor shall conclude subcontracting agreements in writing. This form of requirement is also met if it is in electronic format.

13.3. The Processor shall ensure that the subcontractor(s) are obliged in the subcontracting agreement to provide a standard in writing that does not fall short of the standard agreed herein. Furthermore, the Processor ensures that the responsibilities between Processor and Subcontractor and between multiple subcontractors are clearly delineated. The Processor shall ensure that the Controller is entitled to carry out an appropriate evaluation and inspection with subcontractors, also on site, if necessary, or have these carried out by third parties commissioned by it, unless proof of GDPR compliance can be provided by certification or approval.

13.4. The Processor shall notify the Controller in a timely manner of any intended changes regarding the addition of new or the replacement of previous Subcontractors. The Controller shall have the opportunity to object to these changes for good cause within 14 days. This objection must be in writing and substantiated. Unless approved or objected to within the 14-day period, the relevant Subcontractor shall be deemed approved. If the Controller lawfully objects and the Processor cannot comply with the objection, the Processor shall immediately notify the Controller thereof. Within one month of notification by the Processor, the Controller shall be entitled to terminate the Agreement in writing.

14. Deletion and return of data

14.1. The Processor is prohibited from actively Processing Customer Data after the termination of this Agreement; further storage of the Customer Data only remains permitted until the Processor has provided this Customer Data to the Controller as intended, or deleted or destroyed it; in this case, the provisions of this Agreement shall continue to apply even after termination of the Agreement, until such time as the Processor no longer has any Customer Data.

14.2. The Controller may delete its Customer Data and/or create a copy until the expiration of the contractual relationship only through using the functionality of the META-INF App within its limitations (if the META-INF App grants the possibility thereto). If the META-INF App does not provide the option of deletion for the Controller regarding a specific Customer Data processed by the Processor the Controller may request the deletion of the said Customer Data in writing or in a documented electronic format from the Processor. The Processor shall immediately but within 8 days at the latest delete the Customer Data (including copies and backups) which was requested by the Controller in accordance with the above. After the end of the Agreement, the Processor shall delete all personal Customer Data unless legal requirements require a longer retention period. The data shall then be deleted, no later than 45 days after the end of the Agreement, earlier upon corresponding instructions.

14.3. The Processor is entitled to charge a reasonable fee for cancellation and destruction regarding the processed Customer Data.

15. Entry into force; contract duration and termination

15.1. Present DPA and all its appendixes are effective from the date indicated in the chart contained in Section 1.1. above.

15.2. The duration of the DPA corresponds to the duration of the Agreement. The regulations on the termination of the Agreement apply accordingly. Termination of the Agreement automatically causes termination of this DPA. Termination of this DPA separately and independently is excluded.

15.3. The right of the Parties to extraordinary termination of this DPA and of the Agreement for good cause remains unaffected.

15.4. In case of doubt, a termination of the Agreement also applies as a termination of this DPA.

16. Final Provisions

16.1. Amendments, additions to and the termination of this Agreement must be in writing or agreed upon in a documented electronic format. This also applies to a change or cancellation of the written form requirement.

16.2. The Parties agree that this DPA shall replace any existing DPA the Parties may have previously entered into in connection with the Services.

16.3. If individual provisions of this DPA are or become ineffective or contain a gap, the remaining provisions shall remain unaffected. The Parties undertake to replace the ineffective provision with a legally permissible provision that comes closest to the purpose of the invalid provision and best meets the requirements.

16.4. This DPA is governed by and to be construed in accordance with the GDPR and any other relevant and applicable EU laws and the laws of Hungary. Any and all disputes arising from this DPA shall be governed by the exclusive jurisdiction of the Competent Hungarian Courts based on the Processor's registered seat.