STAMPEDLY

JOINT DATA PROCESSING AGREEMENT

This joint data processing agreement (hereinafter: "Agreement") is established on one part by:

Company name:	Artillence Limited Liability Company
Headquarters:	1124 Budapest, Németvölgyi út 87/A 3rd floor, door 16a.
Company registration number:	Cg.01-09-376748
Tax number:	28848329-2-43
Statistical number:	28848329-6201-113-01.
Represented by:	Karz Gergely Jakab, managing director with independent representation and company signing rights
Phone number:	+36 70 356 3606
E-mail:	info@artillence.com

as the licensor (hereinafter: "Licensor")

on the other part by the

Company name:	
Headquarters:	
Company registration number:	
Tax number:	
Statistical number:	
Represented by:	
Phone number:	
E-mail:	

as the licensee (hereinafter: "Licensee")

(the Licensor and the Licensee hereinafter individually: "Party"; collectively: "Parties") at the place and date written below under the following conditions:

Backgrounds:

(A) The Licensor and the Licensee entered into a software usage agreement on [*] [*]. day of 2023 for the non-exclusive use of the Stampedly digital stamp card service (hereinafter: "Framework Agreement").

(B) Under the Framework Agreement, the Parties process certain personal data (email address) of natural persons using the Stampedly digital stamp card service, which processing is subject to the mandatory provisions of the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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 (hereinafter: "Regulation") applicable from May 25, 2018, under which the Parties are also considered data controllers individually.

(C) The purposes and means of data processing for the performance of the Framework Agreement regarding the Stampedly digital stamp card service are jointly determined by the Parties, therefore they are considered joint data controllers under Article 26 of the Regulation. In order for the Parties to process Personal Data transparently, they define in this Agreement the distribution of their responsibilities regarding the fulfillment of obligations under the Regulation, particularly concerning the exercise of the rights of the data subjects and the provision of information mentioned in Articles 13 and 14 of the Regulation.

(D) The Parties shall apply the Framework Agreement and this Agreement together in order to comply with the provisions of the Regulation.

1. Definitions

1.1. The terms "Data Subject", "Personal Data", "Data Controller", "Data Protection Incident", "Supervisory Authority", "Impact Assessment", and "Data Processor" have the meanings defined in the Regulation.

1.2. In addition, the meanings of the following words and phrases are as follows:

"Responsible Data Controller":	The data controller among the Licensor and the Licensee who, based on the agreement of the Parties, is obliged to perform the tasks outlined in this Agreement in relation to the individual data

	processing activities and to bear the consequences of any omissions.
"Cooperating Data Controller":	A Party that does not qualify as the Responsible Data Controller.
"Infotv.":	Act CXII of 2011 on the right to informational self-determination and freedom of information.

2. The scope of shared Personal Data

2.1. The Parties share the Personal Data specified in Annex 1 of this Agreement for the performance of the Framework Agreement.

3. The rights and obligations of the Parties

3.1. The Parties designate the Licensee as the Responsible Data Controller regarding the joint processing of Personal Data defined in Annex 1 of this Agreement.

3.2. The Responsible Data Controller, as a data controller, is obliged to comply with the provisions of the Regulation applicable to data controllers in several areas, including the following:

a) Ensuring the rights of data subjects, informing the Data Subject

The Responsible Data Controller is obliged to fulfill all obligations towards the Data Subject in accordance with Articles 12-23 of the Regulation.

The information provided under Articles 13 and 14 of the Regulation must be understandable, transparent, and easily accessible. In addition to the provisions of Articles 13 and 14 of the Regulation, the Responsible Data Controller must inform the Data Subject about the joint data processing, the Collaborating Data Controller, the essence of this Agreement, and from whom they can request information about the Personal Data processed under this Agreement and the Framework Agreement, how they can exercise their rights as data subjects, how to file a complaint, under what conditions, and to whom they can turn (contact information) – in accordance with Article 26(3) of the Regulation.

b) Cooperation with the Supervisory Authority

If the Regulation prescribes communication with the Supervisory Authority, the Responsible Data Controller is obliged to comply immediately, including but not limited to the obligations imposed on the Responsible Data Controller by the Regulation in connection with Data Protection Incidents and Impact Assessments.

c) Conducting a data protection review or Impact Assessment

In order to comply with the Regulation, the Responsible Data Controller is obliged to review its data processing processes annually and make modifications as necessary. If the Regulation or its authorization requires the Supervisory Authority to mandate the Responsible Data Controller to conduct an Impact Assessment, the Responsible Data Controller is obliged to carry it out without delay.

d) Data retention obligations

The Responsible Data Controller is obliged to ensure compliance with the data retention requirements set out in the Regulation, the Infotv., and any sectoral or specific national law. In this context, the Responsible Data Controller establishes a data retention procedure and ensures that data processed unnecessarily, without legal basis, or beyond the deadline is deleted or destroyed.

3.3. The Collaborating Data Controller is obliged to provide the Responsible Data Controller with any information necessary for the tasks outlined in point 3.2.

3.4. Both Parties are obliged to comply with the provisions of the Regulation regarding data controllers in several areas, including the following:

a) Proper data management of Personal Data

The Parties are obliged to ensure that they comply with the provisions of the Regulation regarding the processing of Personal Data, including, but not limited to, compliance with the principles set out in the Regulation, and that the processing of Personal Data is carried out based on a precise purpose and appropriate legal basis.

b) Data transfer to a third country or international organization

The Parties are obliged to ensure compliance with the provisions of the Regulation regarding data transfer to a third country or international organization.

c) Data protection register

The Parties are obliged to maintain an up-to-date data protection register of their data processing activities, in accordance with Article 30 of the Regulation.

When determining the appropriate level of security, the Party must specifically take into account the risks arising from data processing, particularly those resulting from the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to Personal Data that is transmitted, stored, or otherwise processed.

d) Confidentiality obligations of employees and third parties (e.g., subcontractors, legal representatives)

The Parties are obliged to ensure that only those individuals who are absolutely necessary for the performance of their tasks as outlined in the Framework Agreement have access to Personal Data. The Parties will take appropriate measures to ensure that individuals acting under their authority and having access to Personal Data can only process such data in accordance with their instructions. The Parties are obliged to ensure that individuals involved in data processing operations receive appropriate levels of data protection training and that their data protection knowledge is kept up to date.

e) Built-in and default data protection, data security

The Parties are obliged to comply with the provisions set out in Article 25 of the Regulation.

The Parties shall implement appropriate technical and organizational measures in accordance with Article 32 of the Regulation, taking into account the state of science and technology and the costs of implementation, as well as the nature, scope, circumstances, and purposes of the data processing carried out in the performance of the Agreement, and the risks of varying likelihood and severity for the rights and freedoms of natural persons, in order to ensure a level of data security appropriate to the risk.

4. Data Protection Incident

4.1. The Parties ensure appropriate security measures and take all technical and organizational security measures regarding Data Protection Incidents affecting Personal Data processed under this Agreement.

4.2. If a Data Protection Incident occurs that is likely to pose a high risk to the rights and freedoms of natural persons, the Party becoming aware of it shall immediately notify the other Party, but no later than 24 hours after becoming aware of such Data Protection Incident, and in such a way that the other Party is also able to comply with the applicable laws regarding Data Protection Incidents, particularly all relevant notification requirements related to Data Protection Incidents and breaches of the security of Personal Data. Notification regarding the Data Protection Incident may generally be made verbally, but must be confirmed in writing.

4.3. The notification must minimally include the items listed in the Regulation, and the Parties are aware of the importance of immediate notification, as well as the tracking and supplementation of previous notifications.

4.4. The Parties must refrain from sharing any information related to the Data Protection Incident with third parties and/or affected individuals in any way, unless they are legally obliged to do so, or if the Parties have agreed otherwise.

5. Cooperation, communication

5.1. The Collaborating Data Controller shall notify the Responsible Data Controller within 24 hours of any requests or inquiries received from the Data Subject or any other third party, including requests for access to Personal Data, rectification, questions regarding data portability, and similar matters. The Collaborating Data Controller shall not respond to such requests unless it has obtained prior consent from the Responsible Data Controller; the Collaborating Data Controller shall cooperate with the Responsible Data Controller in this regard and support the Responsible Data Controller in handling and responding to such complaints, requests, and provisions.

5.2. The Parties shall communicate through the following contacts during the performance of the Agreement:

a) Licensee:
contact person's name: [*]
email address: [*]
phone number: [*]

b) Licensor:
contact person's name: Karz Gergely Jakab
email address: info@artillence.com
phone number: +36 70 356 3606

5.3. The contacts specified above, their address, email address, phone number, and the names and signatures of those authorized to represent the Parties shall be handled by the Parties solely for the purpose of communication and contracting related to the performance of the Agreement, and for taking steps necessary for the performance or conclusion of the Agreement.

5.4. The appropriate legal basis for providing contact details to each other must be ensured by the Party designating the contact person and their contact in their relationship. The Parties declare that they have a proper legal basis for the transfer of data.

5.5. The Parties have a legitimate economic interest in the management of contact and representation data, which is manifested in the fact that it is essential for ensuring the proper performance of the Framework Agreement and this Agreement that the Parties can maintain contact with each other.

5.6. Each Party is obliged to:

a) without undue delay, to notify the other Party in writing of any planned, occurred, or foreseeable changes to any technical, organizational, or financial aspects that may change the legal basis for the transfer of

Personal Data to the other Party or may adversely affect other circumstances;

b) to notify the other Party without undue delay if any data protection authority or other governmental body initiates an investigation regarding the processing of the Personal Data of the Data Subjects. Such notification should be made, if possible and to the extent permitted by applicable laws, before any data provision performed by the Party under investigation.

6. Liability

6.1. If either Party fails to fulfill its obligations under this Agreement, it shall be liable for all damages resulting therefrom.

6.2. The Parties indemnify each other for damages incurred by the other Party, provided that the damage arises from a breach of this Agreement – particularly if damage arises at the Collaborating Data Controller due to the Responsible Data Controller's failure to fulfill its obligations under the Agreement.

6.3. For the purposes of this point, damage means: i) penalties, fines imposed by a court, and other sanctions imposed by a supervisory authority or other government body; ii) compensation claimed by third parties or subcontractors; and iii) reasonable costs related to the implementation of this Section 6.

6.4. The Parties ensure that there is coverage for liability for damages.

7. The Collaborating Data Controller's right to audit

7.1. The Responsible Data Controller maintains a detailed, accurate, and up-to-date record of the processing of Personal Data. The Responsible Data Controller shall provide this record to the Collaborating Data Controller upon request in a manner that does not violate the Responsible Data Controller's business secrets.

7.2. The Collaborating Data Controller is entitled to verify that the measures specified in this Agreement are being implemented.

7.3. The Responsible Data Controller ensures the possibility for the Collaborating Data Controller and its representatives to properly audit data processing:

a) at least 4 times a year, at a time determined by the Collaborating Data Controller - of which the Collaborating Data Controller shall notify the Responsible Data Controller with a 15-day notice period, as well as

b) as necessary in the event of a Data Protection Incident, within a reasonable notification period.

7.4. During the audit, the Collaborating Data Controller shall in all cases respect the Responsible Data Controller's legitimate interest in business secrecy and the continuity of business operations and limit the processing of Personal Data to: i) access to the Responsible Data Controller's information, businesses, and documents; ii) reasonable assistance and support provided by the Responsible Data Controller's employees; and iii) reasonable tools found in the Responsible Data Controller's businesses to examine whether the Responsible Data Controller is fulfilling its obligations under the Agreement.

7.5. The Responsible Data Controller shall change its security policies within a reasonable time based on the reasonable notifications provided by the Collaborating Data Controller regarding audits and inspections and shall modify its data processing procedures as necessary – within reasonable limits.

7.6. Each party bears its own costs for the audits described in this Section 7.

8. Termination of the Agreement

8.1. This Agreement shares the fate of the Framework Agreement and remains in effect until the termination or expiration of the Framework Agreement.

8.2. If the Framework Agreement is terminated, the Agreement shall also automatically terminate; the Agreement – given its nature – cannot be terminated before the expiration of the Framework Agreement or independently of the Framework Agreement.

8.3. If this Agreement is terminated, the Parties are obliged to review whether they are required to delete, destroy, or continue processing the Personal Data in accordance with the provisions of the Regulation. The Party continuing the data processing is solely responsible for any further processing of the Personal Data.

9. Miscellaneous provisions

9.1. The invalidity of any provision of this Agreement does not affect the validity of the other provisions of the Agreement, and the remaining provisions shall remain valid and in effect. The Parties agree to replace the invalid provision with a valid provision that best corresponds to the contractual purpose of the original provision, and if this is not possible, the Agreement shall be interpreted in a manner that best achieves the legal and economic effect intended by the invalid provision, as permitted by law.

9.2. In matters not regulated by this Agreement, the relevant provisions of the Regulation shall apply, including particularly the information and documentation obligations regarding the data controller, and cooperation with authorities.

9.3. In relation to data processing processes not affected by this Agreement, neither Party is responsible for the unlawful data processing activities of the other Party and for bearing any damages arising therefrom.

The Parties signed the Agreement after reading it and mutually agreeing on its interpretation, as a reflection of their will, at the following place and time.

Annex:

1. **Annex No. – The scope of Personal Data processed and the legal basis for data processing**

Budapest, 2023. ______________________________ ____.

____
____
Artillence Ltd. represented by:
Karz Gergely Jakab in
representation based on
authorization:
[*]Licensor Cooperating Data
Controller

_________________________________[*]repre
sented by: Licensee
Responsible Data Processing

1. Annex No.

The scope of Personal Data processed and the legal basis for data processing

Name of the data set	Legal basis for data processing (GDPR)	Responsible data controller
The email address of natural persons using the Stampedly digital stamp card service	Article 6 (1) point a)	Licensee