DATA PROCESSING AGREEMENT

concluded pursuant to Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) and Section 1746(2) of Act No. 89/2012 Coll., the Civil Code

I. Contracting Parties

The Contracting Parties are defined by the General Terms.

II. Introductory Provisions and Subject Matter of the Agreement

1) The Customer acts as the controller of personal data (hereinafter "Personal Data") in relation to all personal data that it itself stores, processes, transmits or otherwise manages through its webhosting, e-mail mailboxes, virtual server (VPS) and/or cloud services (hereinafter the "Services") in connection with the use of the Provider's services.

2) The Provider provides the Services as technical infrastructure and has no obligation or authorisation to acquaint itself with the content of the data that the Customer stores, receives or sends through the Services. The scope of the Provider's role as processor differs for the individual Services and is set out in the annexes to this Agreement (Annex 1 – Webhosting, Annex 2 – E-mail Services, Annex 3 – VPS, Annex 4 – Cloud Services).

3) The purpose of this Agreement is to define the mutual rights and obligations of the Parties in the processing of personal data in accordance with Article 28 GDPR, to the extent corresponding to the technical nature of the Services provided and to the Provider's actual capabilities.

III. Definitions

1) "Personal Data" means any information within the meaning of Article 4(1) GDPR that the Customer stores, processes or transmits through the Services.

2) "Processing" means processing within the meaning of Article 4(2) GDPR.

3) "Content" means data stored, transmitted or processed by the Customer through the Service (files, databases, e-mail messages), whose substance, structure or nature the Provider does not know and does not actively ascertain.

4) "Infrastructure Level" means the technical and organisational security of the platform on which the Services are operated (physical security of the data centre, network security, management of employee access, system-level backup), as distinct from the security or modification of the Content itself.

5) "Service Agreement" means the applicable contractual terms and other documents published at https://www.forpsi.com/agreements/ which the Customer accepted when ordering or renewing the service.

IV. Subject Matter, Nature, Purpose and Duration of Processing

1) The specific subject matter, nature, purpose and duration of the processing, the categories of data subjects and the categories of personal data are specified for the individual Services in Annexes 1–4. The Customer acknowledges that the Provider is unable to determine or verify these categories itself, as it does not perform any content review of the data.

2) The Customer acknowledges that the Provider cannot carry out measures requiring knowledge of the Content, in particular: classification, pseudonymisation, anonymisation or encryption of specific personal data within the Content, or their selective erasure or rectification. The Customer is responsible for such measures at the application/content level.

3) The processing lasts for the term of the Service Agreement for the given Service and ends upon its termination.

4) The Customer's documented instructions within the meaning of Article 28(3)(a) GDPR are the Service Agreement, this Data Processing Agreement and the configuration of the Service made by the Customer in the Provider's user interface / administration. The Provider is entitled, but not obliged, to accept other instructions.

V. Obligations of the Provider as Processor

To the extent that the Provider is a processor under the relevant Annex, it undertakes:

1) To process personal data only on the basis of the Customer's documented instructions under Article IV point 4) and only for the purpose of providing the Service; not to use the Content for any other purpose, in particular not to analyse it, not to copy it beyond what is necessary for the operation and backup of the Service, and not to disclose it to third parties except in the cases provided for in this Agreement or by law.

2) To ensure that persons authorised to process personal data (employees and collaborators of the Provider) have committed themselves to confidentiality or are under a statutory obligation of confidentiality.

3) To adopt appropriate technical and organisational measures pursuant to Article 32 GDPR at the Infrastructure Level, in particular:

    a. physical security of the data centre and control of access to it;

    b. network security, firewall, protection against unauthorised access from outside;

    c. management of the Provider's employees' access rights to the infrastructure;

    d. regular backup at system/platform level according to the standard parameters of the given Service;

    e. recording and monitoring of security incidents at infrastructure level.

4) Within the limits of the technical possibilities described in the Annexes, to assist the Customer in fulfilling its obligation to respond to requests from data subjects under Chapter III GDPR and in fulfilling its obligations under Articles 32–36 GDPR. The Parties agree that this assistance is limited to actions that can be carried out at the Infrastructure Level (e.g. complete deletion of an account or mailbox, provision of an export of the entire Content, or blocking of access) and does not include the identification, search or selective modification of specific personal data within the Content, which only the Customer can carry out.

5) To notify the Customer without undue delay after becoming aware of it of any personal data breach that the Provider detects at the Infrastructure Level (e.g. unauthorised access to the Provider's systems). The Parties acknowledge that the Provider has no technical means of detecting a breach that occurs exclusively at the level of the Customer's Content or application (e.g. a data leak caused by a vulnerability in an application operated by the Customer, compromise of the Customer's access credentials, etc.), and the Provider is not liable for such breaches.

6) To erase all data after the provision of the relevant Service ends; the standard period for erasure after termination is 60 days from the termination of the Service plus 6 days for erasure from backups.

7) To allow the Customer and an auditor mandated by it to carry out an audit or inspection necessary to demonstrate compliance with the obligations under Article 28 GDPR, to a reasonable extent, with at least 30 days' notice, outside normal operating hours and at most once a year, unless it concerns an investigation prompted by a supervisory authority; the costs of the audit are borne by the Customer. The Provider may alternatively fulfil this obligation by presenting a current independent audit/certification.

VI. Obligations and Liability of the Customer as Controller

1) The Customer is responsible for ensuring that all processing of personal data through the Services has a legal basis under Article 6 or Article 9 GDPR, as applicable, and that it gives the Provider only such instructions as comply with the GDPR.

2) The Customer acknowledges and agrees that the Provider does not carry out, and is not obliged to carry out, any content review, classification or filtering of data stored or transmitted through the Services, and that the Customer alone is responsible for determining which personal data are processed through the Services and to what extent.

3) The Customer shall itself ensure, at the level of its Content and its own application logic, such measures (encryption, pseudonymisation, access control, content backup, deletion of specific records, etc.) as correspond to the risks associated with the processing of the personal data it stores.

4) The Customer shall itself handle data subjects' requests to the extent that requires knowledge of the Content, and shall use the Provider's assistance under Article V (assistance with data subjects' requests) for this purpose only to the extent described there.

VII. Relation to VPS, Cloud and Other Unmanaged Services

1) The Parties expressly confirm that, for the Services specified in Annex 3 – VPS and Annex 4 – Cloud Services, the Provider has no access to the data stored, processed or transmitted by the Customer within the virtual server or the virtual infrastructure, except in the situations set out in Annexes 3 and 4.

2) In view of the above, the Parties jointly state that, in relation to the content of the VPS and of the virtual infrastructure, the Provider does not process personal data within the meaning of Article 4(2) GDPR and does not act as a processor; the provisions of this Agreement apply to these Services only mutatis mutandis, to the extent of Annexes 3 and 4, and in particular as a declaration of the scope of access and of the security measures at the Infrastructure Level.

VIII. International Transfers of Data

No personal data are transferred outside the European Economic Area in connection with sub-processors. Information on sub-processors and the location of data centres is provided in Annex 5.

IX. Term and Termination

1) This Data Processing Agreement is concluded for the term of the Service Agreement and is subject to the same term and grounds for termination as the Service Agreement, unless otherwise stated below.

2) Termination of this Agreement does not affect the Provider's obligations under Article V (erasure of data) or the obligation of confidentiality.

X. Final Provisions

1) In the event of a conflict between this Data Processing Agreement and the Service Agreement, this Data Processing Agreement shall prevail in matters of personal data protection.

2) This Agreement is governed by the laws of the Czech Republic. The Parties shall seek to settle any disputes amicably in the first instance.

3) This Agreement takes effect upon acceptance by the Customer and forms an integral part of the Service Agreement.

Annex 1 – Webhosting

Description of the Service	Provision of server space for operating the Customer's websites/applications, including databases.
Scope of the Provider's access	The Provider has the technical ability to access data stored on the hosting (server administration, technical support, backup), but does not actively view the content, except to the extent necessary when resolving a technical problem at the Customer's request or in order to avert an imminent threat to operation.
Nature and purpose of processing	Storage, transmission and backup of data at file-system and database level for the purpose of operating the Customer's website/application.
Categories of data subjects	Determined exclusively by the Customer according to the nature of the application operated (typically e.g. website visitors, e-shop customers, etc.); not known to the Provider.
Categories of personal data	Determined exclusively by the Customer; not known to the Provider, as it does not carry out any content review.
Duration of processing	For the term of the webhosting Service.
Technical measures of the Provider	Server and network security, access control, regular system-level backup according to the plan parameters, encrypted transmission (TLS/SSL) if part of the Service.

Annex 2 – E-mail Services

Description of the Service	Operation of e-mail mailboxes and transmission of the Customer's e-mail messages (receiving, sending, storing).
Scope of the Provider's access	The Provider has the technical ability to access the content of e-mail mailboxes (server administration, technical support), but does not actively view the content, except for automated processing for protection against spam/malware and except to the extent necessary when resolving a technical problem at the Customer's request.
Nature and purpose of processing	Storage, transmission and delivery of e-mail messages and attachments.
Categories of data subjects	Determined exclusively by the Customer (senders and recipients of e-mail communication); not known to the Provider.
Categories of personal data	Determined exclusively by the Customer; the content of messages and attachments may include any personal data as decided by the mailbox users.

Duration of processing	For the term of the e-mail Service, or until the message is deleted by the user.
Technical measures of the Provider	Server and network security, encrypted transmission (TLS), anti-spam and anti-virus checks.

Annex 3 – VPS

Description of the Service	Provision of a virtual server (VPS) under the full management of the Customer, including the operating system and all applications and data that the Customer installs and manages on the VPS itself.
Scope of the Provider's access	The Provider has no access to the operating system, applications or data inside the VPS. The Provider manages only the virtualisation and network infrastructure (hypervisor, network, power supply, physical hardware).
Legal qualification	In relation to the content of the VPS, the Provider is not a processor of personal data within the meaning of Article 4(8) and Article 28 GDPR – see Article VII of this Agreement.
Categories of data subjects and personal data	Not determined – the Provider has neither access to nor knowledge of the content.
Responsibility for the security of the content	Exclusively the Customer (updates of the operating system and applications, firewall configuration at VPS level, content backup, data encryption, management of access credentials).
Technical measures of the Provider	Physical security of the data centre, security of the hypervisor and network infrastructure, separation of individual VPS instances, availability according to the SLA, if one has been concluded. Backup of the VPS content is ensured by the Customer, unless a backup service is expressly agreed in the plan.
Exceptional access by the Provider	The Provider may access the VPS only at the Customer's express request within paid technical support.

Annex 4 – Cloud Services

Description of the Service	Provision of virtual infrastructure and other cloud services (IaaS, PaaS) under the full management of the Customer, including the operating system, the configuration of the virtual infrastructure and all applications and data that the Customer installs and manages in the virtual infrastructure itself.
Scope of the Provider's access	The Provider has no access to the operating system, applications or data inside the virtual infrastructure. The Provider manages only the virtualisation and network infrastructure (hypervisor, network, power supply, physical hardware).

Legal qualification	In relation to the content of the virtual infrastructure, the Provider is not a processor of personal data within the meaning of Article 4(8) and Article 28 GDPR – see Article VII of this Agreement.
Categories of data subjects and personal data	Not determined – the Provider has neither access to nor knowledge of the content.
Responsibility for the security of the content	Exclusively the Customer (updates of the operating system and applications, firewall configuration at the level of the virtual infrastructure, content backup, data encryption, management of access credentials).
Technical measures of the Provider	Physical security of the data centre, security of the hypervisor and network infrastructure, separation of individual instances of the virtual infrastructure, availability according to the SLA, if one has been concluded. Backup of the content of the virtual infrastructure is ensured by the Customer, unless a backup service is expressly agreed in the plan.
Exceptional access by the Provider	The Provider may access the virtual infrastructure only at the Customer's express request within paid technical support.

Annex 5 – List of Sub-processors and Data Centres

Sub-processors	• Aruba S.p.A., Via San Clemente 53 - 24036 Ponte San Pietro, Italy
Data centres	• DC IT1 Arezzo, Italy • DC IT2 Arezzo, Italy • DC IT3 Ponte San Pietro, Italy • DC IT4 Rome, Italy • DC CZ1 Prague, Czech Republic • DC CZ2 Ktiš, Czech Republic • DC FR1 Paris, France • DC DE1 Frankfurt, Germany • DC UK1 London, United Kingdom • DC PL1 Warsaw, Poland