Information on the processing of personal data
pursuant to Art. 13 of the RGPD 679/2016

Dear Madam/Sir,

pursuant to art. 13 of the EU General Data Protection Regulation no. 679/2016, containing provisions on the processing of personal data (hereinafter, **RGPD**), we hereby inform you that **DEFENX ITALIA S.r.**l., as the Data Controller of the data you have provided, will use this information concerning you and, qualified as "personal data" by the RGPD. The regulation states that anyone who processes personal data must inform the person concerned of what data is processed and of certain elements qualifying the processing, which must in any case be carried out in a lawful, correct and transparent manner, protecting your confidentiality and guaranteeing your rights.

1. DATA CONTROLLER

The Data Controller is **DEFENX Italia** Srl, with registered office at Via Larga 7, 20122 Milan.

2. DATA PROTECTION MANAGER (RPD/DPO)

The Data Protection Manager can be contacted at the following email address: dpogruppo@bv-tech.it.

3. PURPOSE OF PROCESSING AND NATURE OF DATA

The information and personal data indicated below will be processed for the following purposes
to fulfil the execution of the contract with you for the supply and management of the following **App**:

- **"Memopal Cloud Backup"**

and/or related services requested by you, namely:

Required data:

a. **user's email address** (required for user identification, registration and login);
b. **user licence key** (required for identification of a specific licence, renewal and support)
c. **account access password** (required to protect access violations);
d. **user's name, model and device type** (required to identify the devices themselves and the features available);
e. **type of operating system** installed in the device referred to in 3d above (necessary to identify the functions available);
f. **IP address** (necessary to protect access violations);
g. **type of browser** (if used) (necessary to identify the available functions);
h. **your files.** The Cloud service automatically archives the files selected by the user;
i. **administrative information** for contract management;

Optional data:

j. **information relating to your request**, if you contact us with questions or complaints;
k. **name and surname** (can be used to identify the user);
l. **residence / domicile address of the user** (can be used to identify the user).

Information on the processing of personal data
pursuant to Art. 13 of the RGPD 679/2016

4. LEGAL BASIS FOR PROCESSING

The personal data referred to in point 3) of the information notice will be processed lawfully because the following conditions are met:

- processing is **necessary for the performance of a contract to which the data subject is party** or for the performance of pre-contractual measures taken at the request of the data subject (art. 6, par.1, letter b RGPD);
- processing is **necessary for the purposes of pursuing the legitimate interests of the Data Controller** (Art. 6(1)(f) GDPR).

5. OBLIGATION OR FACULTY TO PROVIDE DATA AND CONSEQUENCES OF REFUSAL TO DO SO

The provision of data is necessary for the establishment and management of the contractual relationship. We inform you that, in the absence of such data, it will be impossible for our Company to fulfil the obligations of the contract in place with you. Therefore, failure to provide such data will make it impossible to establish or continue the contractual relationship to the extent that such data are necessary for us to correctly fulfil the obligations related to the management of the contract.

Instead, you are free to decide whether or not to provide us with "optional" data. Refusal to provide them will not lead to any detrimental consequences in relation to the existing contractual relationship but will only imply the impossibility of receiving additional services.

6. STORAGE

Personal data will be stored in compliance with the **conservation limitation principle provided** for by the RGPD and / or for the time necessary to pursue the purpose of the service and for legal and / or contractual obligations. In particular:

The data of users with **paid subscription** (as long as the subscription is valid) remain within the infrastructure unless the user requests its deletion. Upon expiry of a paid subscription, or as a result of exercising the right of withdrawal, within 10 (ten) working days following the purchase of the service or the request for deletion of the account, all data is deleted.

The data of users with **free subscription** remain within the infrastructure, unless the user performs any operation for at least 3 (three) years, in this case they will be deleted.

a. **Data recovery in the event of termination or expiration of the Agreement**
   The user can download the archived data for a period of 15 (fifteen) days from the date of termination or expiration of the contract. In the event that 15 days are not sufficient, the user must notify Defenx in writing within this period. In case of receipt of a written request from the user within 15 (fifteen) days of the termination or expiry of the contract, Defenx will be able to send the data on physical support (for example on hard-disk) by post or courier, at the customer's expense.
b. **Data removal**
   At any time, the user can request the cancellation of their data from the archive by written communication. This request will be satisfied within 7 (seven) working days. In the event that the user does not explicitly request cancellation, Defenx may keep the user's data up to a maximum of 90 (ninety) days after the expiry of the contract, exclusively for technical reasons. For the purposes of commercial operations and legal obligations, Defenx will keep the information relating to the customer's account within the terms established by current legislation.

7. SECURITY MEASURES

a. **Digital certificate**
We comply with all industry standard measures aimed at eliminating the risks of damage and unauthorized access or use of personal information, ensuring that we have implemented adequate technical and organizational policies to apply the security measures established by the GDPR. All data is transmitted using the HTTPS protocol encrypted with the TLS (Transport Layer Security) standard at the highest certification level. Any connection to a server that has an untrusted certificate is rejected by the client to avoid Man-in-the Middle-Attack (MITM).
The authentication phase begins only after establishing a valid SSL connection, so that when a fake certificate is offered to the client, no username or password is sent from the client to the server.

b. **Authentication**
To be able to install the solution on any computer, you must have a user account with the appropriate privileges. In this way, no one can install the solution on a PC in order to get hold of other people's data.

c. **Encryption and data**
The data is transferred encrypted from the client to the server, then stored in an encrypted file system and distributed in blocks with the RAID-5 policy.
By inspecting MGFS (Memopal Global File System) it is impossible to know who is the owner of the file being backed up and the name of the original file. If someone were to take a storage unit from the infrastructure, it would still be impossible to access the stored information.
The data structure contains the associations between the files and the owner is also encrypted. These data are not accessible even to service personnel, not even during any maintenance interventions.

d. **Data Center and Server Farm**
The Data Center and the Server Farm are in TIER IV standard (maximum level of certification) and certified according to the ISO 27001 standard. The infrastructure provides, among others, complete fault tolerance, the presence of two electrical power distribution paths simultaneously active and the possibility of carrying out hot maintenance interventions.
The security measures at the physical level of the Data Center include a video surveillance system, perimeter anti-intrusion sensors, armored glass and an armed surveillance station present 7 days a week in 24h mode. The building is designed to be protected against disastrous events of a seismic, energy and hydrological nature.

8. DATA PROCESSING METHODS AND RECIPIENTS

Your personal data will be processed both by the **Company's staff, authorised to process** them using electronic and paper-based instruments, and by **external parties** (collaborators and service providers) called upon to carry out specific tasks on behalf of the Data Controller, in their capacity as **Data Processors**, pursuant to art. 28 RGPD, subject to our letter of appointment imposing on them the duty of confidentiality and security in the processing of personal data, and with the adoption of suitable security measures to prevent loss and/or unlawful and incorrect use of the data and/or unauthorised access, in compliance with the provisions in force on the protection of personal data.

For the sake of brevity, the detailed list of authorized parties, as well as our trusted collaborators and service providers designated as Data Processors, is available at the Data Controller's headquarters and is at your disposal.

8. TRANSFER, DISSEMINATION AND COMMUNICATION OF DATA

The processed data will **not be transferred** to third countries or international organizations, will not be disseminated, and will not be communicated to third parties except, where necessary, for legal and/or contractual obligations.

9. RIGHTS OF THE INTERESTED PARTY

As envisaged by the RGPD, in relation to your data you are entitled to exercise the rights envisaged by articles 15 et seq. of the RGPD, as set out below, and more precisely

- **"right of access"** in order to obtain confirmation from the Data Controller as to whether or not data is being processed personal data concerning you, and if so, to obtain access to the personal data and to the following information: a) to know the purposes of the processing; b) the categories of personal data being processed; c) the recipients or categories of recipients to whom the data have been or will be communicated, in particular if they are recipients from third countries or international organizations; d) where possible, the expected data retention period or the criteria used to determine this period; e) if the data are not collected from the data subject, to obtain all available information on their origin;
- **"right to rectification**" to obtain the rectification of data relating to you;
- **"the "right to erasure/oblivion"** to obtain the erasure of data concerning you in the cases provided for by law;
- **"right to restriction of processing"** to obtain restrictions on processing in the cases provided for by law;
- **"right to data portability"** to obtain the portability of the data, i.e. to receive them from a Data Controller in a structured, commonly used and machine-readable format and to transmit them to another data controller without hindrance in the cases provided for by law;
- **"right to object"** to object to the processing at any time in the cases provided for by law;
- **"right to be informed"** of the existence of an automated decision-making process concerning natural persons, including profiling;
- **"right to lodge a complaint with a Supervisory Authority"** ex art. 77 RGPD (Data Protection Authority).

  Please note that there may be conditions or limitations to the rights of the data subject. It is therefore not certain that, for example, you can exercise your right to data portability in all cases. This depends on the specific circumstances of the processing activity, or, if you decide to object to the processing of your data, the Data Controller has the right to evaluate your request, which may not be accepted if there are compelling legitimate grounds to proceed with the processing that override your interests, rights and freedoms.

10. METHODS OF EXERCISING YOUR RIGHTS

Without any formality, the data subject may at any time exercise his/her rights in a clear and explicit manner by sending:

- an email or **by contacting the DPO/DPO**: dpogruppo@bv-tech.it - +39 02/85.96.171
- by contacting the Controller directly by sending:
  - a registered letter with acknowledgment of receipt to the address **Defenx Italia S.r.l.** Via Larga 7, Milan 20122 Italy
  - an e-mail to: info@defenx.com

Milan 28/03/2022 (last updated)