DATA SECURITY STANDARDS

This Data Security Standard policy (**Policy**) sets forth Humly Solutions AB, co. reg. no. 559233-6480, including all its Affiliates, with address Sveavägen 124, 113 50 Stockholm, Sweden (**Humly**) technical and organizational security measures for the processing of Service data and Personal Data to ensure a level of security appropriate to risks (**Security Standards**).

These Security Standards apply to all Personal data that Humly receives and process while using Humly operated service and Cloud based services and products via hosted online web services (**Services**) and Humly's App.

This Policy also creates the legal framework for Humly's processing of personal data in a manner compliant with EU General Data Protection Regulation 2016/679 (GDPR), and describes how Humly collects, uses, shares, and secures the personal information that You provide. It also describes Your choices regarding use, access, and correction of Your personal information.

CONTACT

If You have questions or complaints regarding this Policy or about Humly's privacy practices, please write to us at data-protection@humly.com.

PSEUDONYMIZATION AND ENCRYPTION

Personal Data handled by Humly shall be encrypted and pseudonymized.

When laptops are used for Personal Data processing, encryption should always take place on fixed and removable storage media.

ACCESS AND ACCESS CONTROL

Humly shall have a technical system for access control to give the right Customer the right access and access. Any such included restriction should be done in such a way that only those who need the tasks to be able to do their work should have access to them.

Humly shall have procedures for how permissions are granted and removed. All access rights must be checked at intervals.

Humly shall have strong authentication checks and routines.

All usernames should be unique and personal.

Password management rules should ensure a high password quality. All authentication information must be stored securely.

PHYSICAL ACCESS CONTROLS

Humly shall take reasonable measures to;

(a) prevent physical access, such as security personnel and secured buildings, and

(b) prevent unauthorized persons from gaining access to Personal Data or ensure third parties operating data centres on its behalf are adhering to such controls.

SYSTEM ACCESS CONTROLS

Humly shall take reasonable measures to prevent Personal Data from being used without authorization. These measures shall vary based on the nature of the Processing undertaken and may include, among other;

(a) controls,

(b) authentication via passwords and/or two-factor authentication,

(c) documented authorization processes,

(d) documented change management processes, and/or,

(e) log of access on several levels.

DATA ACCESS CONTROLS

Humly shall take reasonable measures to provide that;

(a) Personal Data is accessible and manageable only by properly authorized staff,

(b) direct database query access is restricted, and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access, and

(c) Personal Data cannot be read, copied, modified or removed without authorization while Processing.

TRANSMISSION CONTROLS

Humly shall take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of Personal Data by means of data transmission facilities is envisaged so Service Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

INPUT CONTROLS

Humly shall take use commercial best efforts to provide that it is possible to check and establish whether and by whom Service Data has been entered into data processing systems, modified, or removed.

Humly shall take reasonable measures to ensure that;

(a) the Personal Data source is under the control of the Data Controller; and

(b) Personal Data integrated into the Service is managed by secured transmission from Humly for interactions with Humly's User Interface (**UI**) or Application Programming Interface (**API**).

PROTECTION AGAINST MALICIOUS SOFTWARE

Humly shall have active and updated antivirus solutions on the devices used in personal data processing.

Humly shall ensure continuous monitoring of protection against malicious software.

DATA BACKUP

Back-ups of the databases in the Service are taken on a regular basis, are secured, and encrypted to ensure that Personal Data is protected against accidental destruction or loss.

Humly shall have documented procedures for recovery.

Testing of restoration of personal data shall be carried out at intervals and the results documented.

Humly shall have documented procedures for thinning the Personal Data.

LOG

Humly shall ensure that logging of events takes place during all processing activities of the Personal Data. All logs should be checked at intervals.

Humly shall have documented procedures for handling security logs and a system for protecting logs.

LOGICAL SEPARATION

Personal (Service) Data from different Customers and their respective Customer is logically segregated on systems managed by Humly to ensure that Personal Data that is collected by different Customers is segregated from one another.

PHYSICAL SAFETY

Equipment, portable data media and the like that are not under the supervision of the personal data tree shall be locked to be protected against unauthorized use, influence and theft.

PROCEDURES FOR INVESTIGATION

Humly shall ensure that there are both technical and practical prerequisites for investigating suspicions of unauthorized access and other forms of unauthorized use of the Personal Data.

REPAIR AND SERVICE

In the event of repair and service of computer equipment used for processing the Personal Data and performed by someone other than Humly, Humly shall enter into a special confidentiality agreement with the service provider.

At the service provider's visit, service must be done under the supervision of Humly.

-END-