Hosted Data Protection Policy

Bounce Together, hosted by Tsohost, holds data (within the United Kingdom) of our service users. Access is password protected and restricted to named users, with level of access to information on a 'need to know' basis to be able to carry out their job.

The data centre where the solution is hosted, features three 40-rack pods. Each of these is home to 34 servers, as well as two switching and four patching racks. Tsohost has a bespoke 150-metre dark fibre network ring that directly connects to the data centre to the wider internet with its own multi-homed Border Gateway Protocol network, which provides unrivalled connectivity to multiple Tier 1 upstream providers.

In addition - a three-metre-tall perimeter fence, more than 25 CCTV cameras, electronic access control systems and 24/7 personnel are all part of Tsohost security arsenal. Latest cold aisle containment technology is used to regulate the temperature and humidity around the servers. Cool air is delivered to the 'cold aisle' through raised flooring. Servers then draw in the cool air and release it into a 'hot aisle' behind them where it is then recycled.

In the unlikely event of a fire in the data centre, a cleverly programmed INERGEN fire suppression system will kick into action. Deeply effective, it's been specially designed for use in data centre environments. It won't damage hardware or infrastructure when it's deployed. Plus, it doesn't create toxins that are harmful to humans or the environment.

As such Bounce is satisfied with the security levels in place to protect its data.

Security Standards

The standards defined below are in line with the procedures and processes set in place by our chosen hosting providers.

Technical and Organisational Measures

We are committed to protect our customers' information. Taking into account the best practices, the costs of implementation and the nature, scope, circumstances and purposes of processing as well as the different likelihood of occurrence and severity of the risk to the rights and freedoms of natural persons we take the following technical and organisational measures (TOM). When selecting the

measures, **confidentiality**, **integrity**, **availability** and **resilience** are considered. A quick recovery after a physical or technical incident is guaranteed.

Data Privacy Program

Our Data Privacy Program is established to maintain a global data governance structure and secure information throughout its lifecycle. This program is driven by the office of the data protection officer, which oversees the implementation of privacy practices and security measures. We regularly test, assess and evaluate the effectiveness of our Data Privacy Program and Security Standards.

1.1 Confidentiality

Definition: ***"Confidentiality means that personal data is protected against unauthorised disclosure."***

We use a variety of physical and logical measures to protect the confidentiality of our customers' personal data. Those measures include:

1.1.1 Physical Security

- ✔ Physical access control systems in place (Badge access control, Security event monitoring etc.)
- ✔ Surveillance systems including alarms and, as appropriate, CCTV monitoring
- ✔ Clean desk policies and controls in place (Locking of unattended computers, locked cabinets etc.)
- ✔ Visitor Access Management
- ✔ Destruction of data on physical media and documents (shredding, degaussing etc.)

1.1.2 Access Control & Prevention of Unauthorised Access

- ✔ User access restrictions applied, and role-based access permissions provided/reviewed based on segregation of duties principle
- ✔ Strong authentication and authorisation methods (Multi-factor authentication, certificate based authorisation, automatic deactivation/log-off etc.)
- ✔ Centralised password management and strong/complex password policies (minimum
- ✔ length, complexity of characters, expiration of passwords etc.)
- ✔ Controlled access to e-mails and the Internet
- ✔ Anti-virus management
- ✔ Intrusion Prevention System management

1.1.3 Encryption

- ✔ Encryption of external and internal communication via strong cryptographic protocols

- ✔ Encrypting PII/SPII data at rest (databases, shared directories etc.)
- ✔ Full disk encryption for company PCs and laptops
- ✔ Encryption of storage media
- ✔ Remote connections to the company networks are encrypted via VPN
- ✔ Securing the lifecycle of encryption keys
- ✔ Database user credentials for the Bounce application are created and stored using industry-recognised hash/salt cryptography methods.

1.1.4 Data Minimisation

- ✔ PII/SPI minimisation in application, debugging and security logs
- ✔ Pseudonymisation of personal data to prevent directly identification of an individual
- ✔ Segregation of data stored by function (test, staging, live)
- ✔ Logical segregation of data by role based access rights
- ✔ Defined data retention periods for personal data

1.1.5 Security Testing

- ✔ Penetration Testing for critical company networks and platforms hosting personal data
- ✔ Regular network and vulnerability scans

1.2 Integrity

Definition: ***"Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term integrity is used in connection with the term "data", it expresses that the data is complete and unchanged."***

Appropriate change and log management controls are in place, in addition to access controls to be able to maintain the integrity of personal data such as:

1.2.1 Change & Release Management

- ✔ Change and release management process including (impact analysis, approvals, testing, security reviews, staging, monitoring etc.)
- ✔ Role & Function based (Segregation of Duties) access provisioning on production environments

1.2.2 Logging & Monitoring

- ✔ Logging of access and changes on data

- ✔ Centralised audit & security logs
- ✔ Monitoring of the completeness and correctness of the transfer of data (end-to-end check)

1.3 Availability

Definition: "The availability of services and IT systems, IT applications, and IT network functions or of information is guaranteed, if the users are able to use them at all times as intended."

We implement appropriate continuity and security measures to maintain the availability of its services and the data residing within those services:

- ✔ Regular fail-over tests applied for critical services
- ✔ Extensive performance/availability monitoring and reporting for critical systems
- ✔ Incident response programme
- ✔ Critical data either replicated or backed up (Cloud Backups/Hard Disks/Database replication etc.)
- ✔ Planned software, infrastructure and security maintenance in place (Software updates, security patches etc.)
- ✔ Redundant and resilient systems (server clusters, mirrored DBs, high availability setups etc.) located on off-site and/or geographically separated locations
- ✔ Use of uninterruptible power supplies, fail redundant hardware and network systems
- ✔ Alarm, security systems in place
- ✔ Physical Protection measures in place for critical sites (surge protection, raised floors, cooling systems, fire and/or smoke detectors, fire suppression systems etc.)
- ✔ DDOS protection to maintain availability
- ✔ Load & Stress Testing

1.4 Data Processing Instructions

Definition: "Data Processing Instructions refers to ensuring that personal data will only be processed in accordance with the instructions of the data controller and the related company measures"

We have established internal privacy policies, agreements and conduct regular privacy trainings for employees to ensure personal data is processed in accordance with customers' preferences and instructions.

- ✔ Privacy and confidentiality terms in place within employee contracts
- ✔ Regular data privacy and security trainings for employees
- ✔ Appropriate contractual provisions to the agreements with sub-contractors to maintain instructional control rights
- ✔ Regular privacy checks for external service providers
- ✔ Providing customers full control