BEAMERY

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

.

Measure	Description
Measures of pseudonymisation and encryption of personal data	Industry standard encryption technologies for Personal Data that is: (i) transmitted over public networks (*i.e.*, the Internet) or when transmitted wirelessly; or (ii) at rest. Supplier encrypts data in transit in accordance with TLS 1.2 or above and at rest in accordance with AES256.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Organisational management and dedicated staff responsible for the development, implementation and maintenance of Processor's information security program. Data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g., role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for Personal Data, as described above. Network security controls that provide for the use of stateful firewalls and layered DMZ architectures and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack. Vulnerability assessment, patch management and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Incident / problem management procedures designed to allow Processor to investigate, respond to, mitigate and notify of events related to Processor's technology and information assets.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Processor's organisation, monitoring and maintaining compliance with Processor's policies and procedures, and reporting the condition of its information security and compliance to internal senior management.
Measures for user identification and authorisation	Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur). Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Processor's passwords that are assigned to its employees: (i) be at least ten (10) characters in length, (ii) not be stored in readable format on Processor's computer systems, (iii) must have defined complexity, and (iv) must have a history threshold to prevent reuse of recent passwords. Multi-factor authentication, where available, must always be used.
Measures for the protection of data during transmission	Industry standard encryption technologies for Personal Data that is transmitted over public networks (*i.e.*, the Internet) or when transmitted wirelessly.
Measures for the protection of data during storage	Supplier encrypts data at rest in accordance with AES256. Backup files are encrypted at rest and in transit between primary and secondary storage locations.

Measures for ensuring physical security of locations at which personal data are processed	Physical and environmental security of data center, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorised physical access, (ii) manage, monitor and log movement of persons into and out of Processor facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.
Measures for ensuring events logging	System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.
Measures for ensuring system configuration, including default configuration	Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Processor's possession.
Measures for internal IT and IT security governance and management	Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to Processor's technology and information assets.
Measures for certification/assurance of processes and products	Organisational management and dedicated staff responsible for the development, implementation and maintenance of Processor's information security program.
Measures for ensuring data minimisation	Not applicable to Processor. Processor is processing the Personal Data on behalf of the Controller for the sole purpose of providing services to the Processor for the duration of the services agreement entered into between the Processor and the Controller. The Controller has complete control over the collection, modification, and deletion of Personal Data (subject to the data retention section, below).

Measures for ensuring data quality	Not applicable to Processor. Processor is processing the Personal Data on behalf of the Controller for the sole purpose of providing services to the Processor for the duration of the services agreement entered into between the Processor and the Controller. The Processor does not have the ability to monitor the quality of the Personal Data.
Measures for ensuring limited data retention	The Controller is permitted to set its own retention rules per a dedicated feature within the application and can self-service delete the personal data it has collected at any point during the term of the underlying Agreement. All Personal Data in the Controller's account is automatically deleted ninety (90) days following expiration or termination of the services agreement entered into between the Controller and Processor, or earlier upon request, subject to the Processor's standard 30 day backup schedule.
Measures for ensuring accountability	The Processor takes responsibility for complying with the EU GDPR and the UK GDPR, at the highest management level and throughout our organisation. The Processor keeps evidence of the steps taken to comply with the EU GDPR and the UK GDPR. The Processor puts in place appropriate technical and organisational measures, such as: (i) adopting and implementing data protection policies (where proportionate), (ii) putting written contract in place with organisations that process personal data on our behalf, (iii) maintaining documentation of our processing activities, (iv) implementing appropriate security measures, (v) recording and, where necessary, reporting personal data breaches, and (vi) carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests. We review and update our accountability measures at appropriate intervals.

Measures for allowing data portability and ensuring erasure	Controller's data can be exported in CSV format at any time. Controller's data is retained as long as the contract is active and is securely deleted from production within 30 days of contract termination and within further 90 days from backups. Media and equipment assets are disposed of securely using NIST SP 800-88/DoD 5220.22-M approved destruction standards. The disposal of printed materials must be witnessed secure shredding and placed in locked secure disposal bins.