ANNEX B

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Technical and organizational security measures to be implemented by inSided (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks to the rights and freedoms of natural persons:

A. ANNUAL EVIDENCE OF COMPLIANCE

1. **Third Party Security Audit.** inSided shall continue to be annually audited against the SOC 2 Type II or ISO 27001 standard (the "***Security Standard***"). All such audits shall be conducted by an independent third party auditor and at inSided's expense. The audit shall be completed by an independent third party. Upon Client's written request to security@insided.com, inSided will provide a copy of the resulting annual audit report (the "***Annual Security Report***"). Although the Annual Security Report provides an independently audited confirmation of inSided's security posture, the most common points of interest are further detailed below. inSided shall provide Client with this initial evidence of compliance within 30 days of written request and annually upon written request.

2. **Executive Summary of Web Application Penetration Test.** inSided shall continue to annually engage an independent, third party to perform a web application penetration test. Upon Client's written request to security@insided.com, inSided shall provide the executive summary of the report to Client. inSided shall address all vulnerabilities in the findings of the report within a reasonable, risk-based timeframe. inSided shall provide Client with this initial evidence of compliance within 30 days of written request and annually upon written request.

B. SECURITY

1. Process-Level Requirements.

- inSided shall implement user termination controls that include access removal/disablement promptly upon termination of staff.
- inSided shall provide, and ensure completion of, annual Security Awareness training to all employees.

2. Network Requirements.

- inSided shall use firewall(s), Security Groups/VPCs, or similar technology to protect servers storing Client Data.
- inSided shall ensure that vulnerability scans are completed at minimum quarterly using an industry standard vulnerability scanning tool. All cloud hosted systems shall be scanned, where

applicable and where approved by the cloud service provider. Findings shall be addressed within a reasonable, risk-based timeframe.

3. Hosting Requirements.

- Where inSided handles Client Data, servers shall be protected from unauthorized access with appropriate physical security mechanisms. These physical security mechanisms may be provided by data center partners such as, but not limited to, AWS, Salesforce, and Google.
- Two-factor or two-step authentication is required for any interface which
    i. Allows access to stored Client Content,
    ii. Only receives interactive logins, and
    iii. Faces the open Internet (source traffic isn't restricted by source address).
- inSided will virtually segregate all Client Data in accordance with its established procedures. Client's instance of the Subscription Services may be on servers used by other non-Client instances.

4. APPLICATION-LEVEL REQUIREMENTS.

- inSided shall maintain documentation on overall application architecture, process flows, and security features for applications handling Client Data.
- inSided shall employ secure programming techniques and protocols in the development of applications handling Client Data.
- inSided shall employ scanning tools or other techniques to identify application vulnerabilities prior to all major releases.

5. DATA-LEVEL REQUIREMENTS.

- Encryption and hashing protocols used for Client Data in transit and at rest shall support NIST approved encryption standards (e.g. TLS 1.2 or higher).
- inSided shall ensure laptop disk encryption.
- inSided shall ensure that access to information and application system functions is restricted to authorized personnel only.
- Client Data stored on archive or backup systems shall be stored at the same level of security or better than the data stored on operating systems.
- inSided shall have a process in place to ensure that secure data is properly deleted.
- Data will be deleted within the post-termination time frame set forth in the Agreement. A 90-day window is designated to account for any backup data retention.

6. END USER COMPUTING LEVEL REQUIREMENTS.

- inSided shall employ an endpoint security solution for laptops used to handle Client Data.
- inSided will have a policy to prohibit the use of removable media (including flash drives, CDs and DVDs) for storing or carrying Client Data.

7. COMPLIANCE REQUIREMENTS.

- inSided shall adopt appropriate physical, technical and organizational security measures in accordance with industry standards, including but not limited to building access control and employee security awareness education.
- inSided will, when and to the extent legally permissible, perform criminal background verification checks on all of its employees that assist in the delivery of Services to Client prior to obtaining access to Client Data. Such background checks shall be carried out in accordance with relevant laws, regulations, and ethics.
- inSided will maintain an Information Security Policy (ISP) that is reviewed and approved annually at the executive level.

8. SHARED RESPONSIBILITY.

The Subscription Services require a shared responsibility model. For example, Client must maintain controls over Client user accounts (such as disabling/removing access when a Client employee is terminated, establishing password requirements for Client users, etc.).

9. SPECIFIC MEASURES.

Measure	**Description**
Measures of encryption of personal data	inSided has taken the following measures in the Services designed to convert clearly legible Client Data into ciphertext by means of a cryptographic process: ● Client Data transmitted via TLS can be encrypted with TLS 1.2 or stronger alternative supported. ● Client Data at rest is encrypted by default using AES256 or a stronger alternative.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Confidentiality: inSided has taken the following measures designed to ensure that Client Data is accessed only by authorized personnel and prevents the intrusion by unauthorized persons into inSided's systems and applications used for the processing of Client Data: ● Multi/Two Factor Authentication and Encryption: ● Two factor or two step authentication is required as described above.

	● All Client Data is subject to the encryption measures identified above. ● Security and Privacy Awareness Training: ● All inSided personnel participate in annual Security and Privacy Awareness training. <u>General:</u> ● Dev/Test environments are separate from production environments by design. ● inSided maintains administrative controls which govern access under the principle of least privilege. ● Safeguards regarding system access: ● Background screening of personnel is carried out as described above. ● Privileged access is not granted by default. <u>Integrity:</u> inSided has taken the following measures designed to ensure that Client Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish whether and by whom Client Data has been input into data processing systems, modified or removed: ● All Client Data is subject to the encryption measures identified above. ● The inSided Security and Operations Teams have tools in place for audit trails, event notifications, and logs for application and cloud systems. <u>Availability and Resilience:</u> inSided has taken the following measures designed to ensure that Client Data is protected from accidental destruction or loss due to internal or external influences, and ensure the ability to withstand attacks or to quickly restore systems to working order after an attack): ● Alerting is set up for specified thresholds and a 24x7 NOC team monitors system availability and overall health. ● High availability clustering is used as appropriate to increase availability. ● The inSided Operations Team ensures routine backups are taken of production systems.
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	inSided has taken the following measures designed to ensure the possibility to quickly restore the inSided system or Client Data in the event of a physical or technical incident: inSided maintains an Incident Response Plan (IRP) that it updates from time to time as needed. The IRP includes procedures for handling and reporting incidents including detection and reaction to possible Security Incidents. ● The inSided Operations Team ensures routine backups of productions

	systems are taken. ● Capacity management measures are taken to monitor resource consumption of systems as well as planning of future resource requirements.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	inSided has taken the following measures designed to ensure the regular review and assessment of security measures: ● As described in *Section A (Annual Evidence of Compliance)* above.
Measures for user identification and authorisation	inSided has taken the following measures designed to validate and authenticate users: ● inSided maintains administrative controls which govern access under the principle of least privilege. ● Access to non-public inSided data or functionality requires authentication prior to access. ● Two factor or two step authentication is required as described above.
Measures for the protection of data during transmission	inSided has taken the following measures designed to ensure transmission control to ensure that Client Data cannot be read, copied, changed or deleted without authorization during its transfer and that Client Data can be monitored and determined to which recipients a transfer of Client Data is intended: ● Client Data is encrypted in transit as described above.
Measures for the protection of data during storage	inSided has taken the following control measures designed to ensure that Client Data cannot be read, copied, changed or deleted without authorization while stored on data media: ● Client Data is encrypted at rest as described above. ● Two factor or two step authentication is required as described above.
Measures for ensuring physical security of locations at which personal data are processed	inSided has taken the measures identified above regarding the physical security of Client Data.
Measures for ensuring events logging	inSided has taken the following measures designed to ensure the verifiability of event log files: ● Remote logging. ● inSided maintains administrative controls which govern access under the principle of least privilege.
Measures for ensuring system configuration, including default configuration	inSided has taken the following measures designed to ensure that all in-scope systems and devices are compliant with baseline configuration settings: ● inSided ensures that access to information and application system functions is restricted to authorized personnel only. ● Baseline configuration identification.

Measures for internal IT and IT security governance and management	inSided has a dedicated and identified person to oversee its information security and compliance program. ● As noted in *Section A.1 (Third Party Security Audit)* above, inSided is annually audited by an independent third-party against the Security Standard.
Measures for certification/assurance of processes and products	● As noted in *Section A.1 (Third Party Security Audit)* above, inSided is annually audited by an independent third-party against the Security Standard.
Measures for ensuring data minimisation	inSided has taken the following measures designed to reduce the amount of data collected by the Subscription Services: ● Provide capabilities for Client to customize which data is collected by the Subscription Services.
Measures for ensuring data quality	inSided has taken the following measures designed to ensure that the data pipeline creates and sustains good data quality: ● inSided has established processes for data subjects to exercise their data protection rights (right to amend and update information). ● inSided's documentation clearly states the types of data Client is prohibited from transferring to inSided.
Measures for ensuring limited data retention	● inSided has established processes designed to ensure that Client Data is deleted in accordance with the terms of the Agreement following the termination of the Agreement.
Measures for ensuring accountability	● inSided has an appointed Data Protection Officer (DPO) who is responsible for overseeing inSided's compliance with its legal and contractual privacy-related obligations throughout the data lifecycle. ● The DPO performs data protection impact assessments for any new processing initiative involving Client Data.
Measures for allowing data portability and ensuring erasure	● inSided has established processes in relation to the exercise by users of their privacy rights (including without limitation, rights of data portability and erasure) in order for inSided to comply with ***Section 9.1*** of the DPA.