

**ANNEX B**

**TECHNICAL AND ORGANISATIONAL SECURITY MEASURES**

Technical and organizational security measures to be implemented by Gainsight (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.** Gainsight shall continue to be annually audited against the SOC 2 Type II and/or ISO 27001 standard (the "**Security Standard**"). All such audits shall be conducted by an independent third party auditor and at Gainsight's expense. The audit shall be completed by an independent third party. Upon Client's written request to security@gainsight.com, Gainsight 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 Gainsight's security posture, the most common points of interest are further detailed below. Gainsight 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.** Gainsight shall continue to annually engage an independent, third party to perform a web application penetration test. Upon Client's written request to security@gainsight.com, Gainsight shall provide the executive summary of the report to Client. Gainsight shall address all vulnerabilities in the findings of the report within a reasonable, risk-based timeframe. Gainsight 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.**

- Gainsight shall implement user termination controls that include access removal/disablement promptly upon termination of staff.
- Documented change control process will be used to record and approve all major releases in Gainsight's environment for all Subscription Services.
- Gainsight shall have and maintain a patch management process to implement patches in a reasonable, risk-based timeframe.
- Gainsight shall provide, and ensure completion of, annual Security Awareness training to all employees.

### **2. Network Requirements.**

- Gainsight shall use firewall(s), Security Groups/VPCs, or similar technology to protect servers storing Client Data.

- Gainsight 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 Gainsight 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).
- Gainsight 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.**

- Gainsight shall maintain documentation on overall application architecture, process flows, and security features for applications handling Client Data.
- Gainsight shall employ secure programming techniques and protocols in the development of applications handling Client Data.
- Gainsight 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).
- Gainsight shall ensure laptop disk encryption.
- Gainsight 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.
- Gainsight 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.**

- Gainsight shall employ an endpoint security solution for laptops used to handle Client Data.
- Gainsight 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.**

- Gainsight 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.
- Gainsight 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.
- Gainsight 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.**

<u>Measure</u>	<u>Description</u>
<b>Measures of encryption of personal data</b>	<p>Gainsight has taken the following measures in the Services designed to convert clearly legible Client Data into ciphertext by means of a cryptographic process:</p> <ul style="list-style-type: none"> <li>● Client Data transmitted via TLS can be encrypted with TLS 1.2 or stronger alternative supported.</li> <li>● Client Data at rest is encrypted by default using AES256 or a stronger alternative.</li> </ul> <p><u>A Note on Email:</u></p> <ul style="list-style-type: none"> <li>● The Services may include inbound and outbound functionality over email. Although Gainsight makes efforts to encrypt data sent over email, such encryption of email cannot be guaranteed.</li> </ul>
<b>Measures for ensuring ongoing confidentiality, integrity, availability</b>	<u>Confidentiality:</u>

**and resilience of processing systems and services**

Gainsight 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 Gainsight'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 Gainsight personnel participate in annual Security and Privacy Awareness training.

General:

- Dev/Test environments are separate from production environments by design.
- Gainsight 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.

Integrity:

Gainsight 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 Gainsight Security and Operations Teams have tools in place for audit trails, event notifications, and logs for application and cloud systems.

Availability and Resilience:

Gainsight 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 Gainsight Operations Team ensures routine backups are taken of

	production systems.
<b>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</b>	<p>Gainsight has taken the following measures designed to ensure the possibility to quickly restore the Gainsight system or Client Data in the event of a physical or technical incident:</p> <ul style="list-style-type: none"> <li>• Gainsight 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.</li> <li>• The Gainsight Operations Team ensures routine backups of production systems are taken.</li> <li>• Capacity management measures are taken to monitor resource consumption of systems as well as planning of future resource requirements.</li> </ul>
<b>Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing</b>	<p>Gainsight has taken the following measures designed to ensure the regular review and assessment of security measures:</p> <ul style="list-style-type: none"> <li>• In addition to the measures identified in <b>Section A (Annual Evidence of Compliance)</b> above, Gainsight also manages a “bug bounty” program for all Subscription Services to allow security researchers to assist in identifying security vulnerabilities in such Subscription Services.</li> </ul>
<b>Measures for user identification and authorisation</b>	<p>Gainsight has taken the following measures designed to validate and authenticate users:</p> <ul style="list-style-type: none"> <li>• Gainsight maintains administrative controls which govern access under the principle of least privilege.</li> <li>• Access to non-public Gainsight data or functionality requires authentication prior to access.</li> <li>• Two factor or two step authentication is required as described above.</li> </ul>
<b>Measures for the protection of data during transmission</b>	<p>Gainsight 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:</p> <ul style="list-style-type: none"> <li>• Client Data is encrypted in transit as described above.</li> </ul>

<p><b>Measures for the protection of data during storage</b></p>	<p>Gainsight 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:</p> <ul style="list-style-type: none"> <li>• Client Data is encrypted at rest as described above.</li> <li>• Two factor or two step authentication is required as described above.</li> </ul>
<p><b>Measures for ensuring physical security of locations at which personal data are processed</b></p>	<p>Gainsight has taken the measures identified above regarding the physical security of Client Data.</p>
<p><b>Measures for ensuring events logging</b></p>	<p>Gainsight has taken the following measures designed to ensure the verifiability of event log files:</p> <ul style="list-style-type: none"> <li>• Remote logging.</li> <li>• Gainsight maintains administrative controls which govern access under the principle of least privilege.</li> </ul>
<p><b>Measures for ensuring system configuration, including default configuration</b></p>	<p>Gainsight has taken the following measures designed to ensure that all in-scope systems and devices are compliant with baseline configuration settings:</p> <ul style="list-style-type: none"> <li>• Gainsight ensures that access to information and application system functions is restricted to authorized personnel only.</li> <li>• Baseline configuration identification.</li> </ul>
<p><b>Measures for internal IT and IT security governance and management</b></p>	<ul style="list-style-type: none"> <li>• Gainsight has a dedicated and identified person to oversee its information security and compliance program.</li> <li>• As noted in <b>Section A.1 (Third Party Security Audit)</b> above, Gainsight is annually audited by an independent third-party against the Security Standard</li> </ul>
<p><b>Measures for certification/assurance of processes and products</b></p>	<ul style="list-style-type: none"> <li>• As noted in <b>Section A.1 (Third Party Security Audit)</b> above, Gainsight is annually audited by an independent third-party against the Security Standard.</li> </ul>
<p><b>Measures for ensuring data minimisation</b></p>	<p>Gainsight has taken the following measures designed to reduce the amount of data collected by the Subscription Services:</p> <ul style="list-style-type: none"> <li>• Provide capabilities for Client to customize which data is collected by the Subscription Services.</li> </ul>
<p><b>Measures for ensuring data quality</b></p>	<p>Gainsight has taken the following measures designed to ensure that the data pipeline creates and sustains good data quality:</p> <ul style="list-style-type: none"> <li>• Gainsight has established processes for data subjects to exercise their data protection rights (right to amend and update information).</li> <li>• Gainsight’s documentation clearly states the types of data Client is prohibited from transferring to Gainsight.</li> </ul>

<p><b>Measures for ensuring limited data retention</b></p>	<ul style="list-style-type: none"> <li>● Gainsight 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.</li> </ul>
<p><b>Measures for ensuring accountability</b></p>	<ul style="list-style-type: none"> <li>● Gainsight has an appointed Data Protection Officer (DPO) who is responsible for overseeing Gainsight’s compliance with its legal and contractual privacy-related obligations throughout the data lifecycle.</li> <li>● The DPO performs data protection impact assessments for any new processing initiative involving Client Data.</li> </ul>
<p><b>Measures for allowing data portability and ensuring erasure</b></p>	<ul style="list-style-type: none"> <li>● Gainsight 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 Gainsight to comply with <b>Section 9.1</b> of the DPA.</li> </ul>



**ANNEX C**  
**SUB-PROCESSOR LIST**

**INSIDED SUB-PROCESSORS**

<b>Name:</b>	Amazon Web Services, Inc.
<b>Address:</b>	410 Terry Ave. North Seattle, WA 98109-5210
<b>Contact Person's Name, Position and Contact Details:</b>	Steve Schmidt, Chief Information Security Officer Compliance Support Form (online AWS.amazon.com)
<b>Description of Processing:</b>	Cloud Service Provider
<b>Location(s) of Processing Activities:</b>	U.S.A.
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	Amazon Web Services EMEA SARL
<b>Address:</b>	Two Park Place, Hatch Street, Dublin 2 Ireland
<b>Contact Person's Name, Position and Contact Details:</b>	Steve Schmidt, Chief Information Security Officer Compliance Support Form (online AWS.amazon.com)
<b>Description of Processing:</b>	Cloud Service Provider
<b>Location(s) of Processing Activities:</b>	Ireland
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	Google, LLC
<b>Address:</b>	1600 Amphitheatre Parkway, Mountain View, CA 94043
<b>Contact Person's Name, Position and Contact Details:</b>	Emil Ochotta, Data Privacy Officer Support@Google.com
<b>Description of Processing:</b>	Back-up Cloud Service Provider and Data Analytics provider
<b>Location(s) of Processing Activities:</b>	U.S.A.
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	Google Cloud EMEA Limited
<b>Address:</b>	Velasco, Clanwilliam Place, Dublin 2, Ireland
<b>Contact Person's Name, Position and Contact Details:</b>	Emil Ochotta, Data Privacy Officer Support@Google.com
<b>Description of Processing:</b>	Back-up Cloud Service Provider
<b>Location(s) of Processing Activities:</b>	the Netherlands
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	Algolia
<b>Address:</b>	For Non-EU Inquiries: 301 Howard Street, 3 <sup>rd</sup> Floor San Francisco, CA 94105 For EU Inquiries: 55 Rue d'Amsterdam 75008 Paris, France
<b>Contact Person's Name, Position and Contact Details:</b>	Adanech Getachew, General Counsel privacy@algolia.com
<b>Description of Processing:</b>	Data Host for search capabilities
<b>Location(s) of Processing Activities:</b>	Germany
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

## OTHER SUBSCRIPTION SERVICES' SUB-PROCESSORS

### Infrastructure Sub-processors

<b>Name:</b>	Salesforce.com, Inc.
<b>Address:</b>	415 Mission Street, 3rd Floor San Francisco, CA 94105
<b>Contact Person's Name, Position and Contact Details:</b>	Lindsey Finch, Data Privacy Officer, privacy@salesforce.com
<b>Description of Processing:</b>	Cloud Service Provider
<b>Location(s) of Processing Activities:</b>	U.S.A. and Germany
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	Heroku
<b>Address:</b>	415 Mission Street, 3rd Floor San Francisco, CA 94105
<b>Contact Person's Name, Position and Contact Details:</b>	Lindsey Finch, Data Privacy Officer, privacy@salesforce.com
<b>Description of Processing:</b>	Cloud Service Provider
<b>Location(s) of Processing Activities:</b>	U.S.A. and Germany
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	Amazon Web Services, Inc.
<b>Address:</b>	410 Terry Ave. North Seattle, WA 98109-5210
<b>Contact Person's Name, Position and Contact Details:</b>	Steve Schmidt, Chief Information Security Officer Compliance Support Form (online AWS.amazon.com)
<b>Description of Processing:</b>	Cloud Service Provider for Gainsight CS Product only
<b>Location(s) of Processing Activities:</b>	U.S.A. and Germany
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	Google, LLC
<b>Address:</b>	1600 Amphitheatre Parkway Mountain View, CA 94043
<b>Contact Person's Name, Position and Contact Details:</b>	Emil Ochotta, Data Privacy Officer Support@Google.com
<b>Description of Processing:</b>	Cloud Computing for Gainsight PX product only, Web Services
<b>Location(s) of Processing Activities:</b>	U.S.A. and Germany
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	Sendgrid, Inc.
<b>Address:</b>	1401 Walnut, Suite 500 Boulder, CO 80302
<b>Contact Person's Name, Position and Contact Details:</b>	Michael Tognetti, Sr. VP, General Counsel legal@sendgrid.com
<b>Description of Processing:</b>	Email Service Provider
<b>Location(s) of Processing Activities:</b>	U.S.A.
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	IBM Watson
<b>Address:</b>	1101 Kitchawan Rd. Yorktown Heights, NY 10598
<b>Contact Person's Name, Position and Contact Details:</b>	Christina Montgomery, Chief Privacy Officer chiefprivacyoffice@ibm.com
<b>Description of Processing:</b>	Natural Language Processing and Cloud Service Provider for Gainsight CX Product only
<b>Location(s) of Processing Activities:</b>	U.S.A.
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	Auth0, Inc.
<b>Address:</b>	10800 NE 8th Street, Suite 700 Bellevue, WA 98004
<b>Contact Person's Name, Position and Contact Details:</b>	Lucy McGrath, Vice President, Privacy privacy@auth0.com
<b>Description of Processing:</b>	Description of processing: Authentication Platform
<b>Location(s) of Processing Activities:</b>	U.S.A. and Germany
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	Sumologic, Inc.
<b>Address:</b>	350 Main Street Redwood City, CA 94063

<b>Contact Person's Name, Position and Contact Details:</b>	Glenn Watt, Chief Information Security Officer privacy@sumologic.com
<b>Description of Processing:</b>	Log Management and Analytics
<b>Location(s) of Processing Activities:</b>	U.S.A. and Germany
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	UiPath (successor in interest to Cloud Elements)
<b>Address:</b>	3858 Walnut Street, Suite 235 Denver, CO 80205
<b>Contact Person's Name, Position and Contact Details:</b>	Ed Fuller, Chief Information Security Officer privacy@uipath.com
<b>Description of Processing:</b>	iPaaS
<b>Location(s) of Processing Activities:</b>	U.S.A. and Ireland
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

#### **Infrastructure Sub-processors**

<b>Name:</b>	Zendesk, Inc.
<b>Address:</b>	989 Market Street San Francisco, CA 94103
<b>Contact Person's Name, Position and Contact Details:</b>	Shanti Ariker, General Counsel privacy@zendesk.com
<b>Description of Processing:</b>	Customer Service Software
<b>Location(s) of Processing Activities:</b>	U.S.A.
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	Box, Inc.
<b>Address:</b>	900 Jefferson Avenue Redwood City, CA 94063
<b>Contact Person's Name, Position and Contact Details:</b>	Paul Chapman, Chief Information Officer dpo@box.com
<b>Description of Processing:</b>	Content Management and File Sharing
<b>Location(s) of Processing Activities:</b>	U.S.A.
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

#### **Gainsight Affiliate Sub-processors**

<b>Name:</b>	Gainsight Software Private Limited (India)
<b>Address:</b>	350 Bay Street, Suite 100 San Francisco, CA 94133
<b>Contact Person's Name, Position and Contact Details:</b>	Anil Chalasani, EVP, Managing Director - India, privacy@gainsight.com

	With a copy to: Dave Swarthout, DPO privacy@gainsight.com
<b>Description of Processing:</b>	Assist in delivery of some or all of the Services
<b>Location(s) of Processing Activities:</b>	India
<b>GDPR Transfer Mechanism:</b>	Standard Contractual Clauses (SCCs)

<b>Name:</b>	Gainsight UK LTD.
<b>Address:</b>	350 Bay Street, Suite 100 San Francisco, CA 94133
<b>Contact Person's Name, Position and Contact Details:</b>	Dave Swarthout, Director privacy@gainsight.com
<b>Description of Processing:</b>	Assist in delivery of some or all Services
<b>Location(s) of Processing Activities:</b>	England
<b>GDPR Transfer Mechanism:</b>	Adequacy Decision

<b>Name:</b>	Aprinsic, Ltd.
<b>Address:</b>	350 Bay Street, Suite 100 San Francisco, CA 94133
<b>Contact Person's Name, Position and Contact Details:</b>	Dave Swarthout, Director privacy@gainsight.com
<b>Description of Processing:</b>	Assist in delivery of some or all Services relating to the Gainsight PX product
<b>Location(s) of Processing Activities:</b>	Israel
<b>GDPR Transfer Mechanism:</b>	Adequacy Decision

<b>Name:</b>	inSided B.V.
<b>Address:</b>	Singel 118A, 1015 AE Amsterdam The Netherlands
<b>Contact Person's Name, Position and Contact Details:</b>	Dave Swarthout, Vice President privacy@insided.com
<b>Description of Processing:</b>	Assist in delivery of some or all Services relating to the inSided Subscription Services
<b>Location(s) of Processing Activities:</b>	The Netherlands
<b>GDPR Transfer Mechanism:</b>	N/A