

PRIVACY SCHEDULE

This Privacy Schedule ("**Privacy Schedule**") forms part of the Agreement between LevelBlue and Client, and any applicable Order Form or SOW. To the extent that the provisions of this Privacy Schedule conflict with, or are inconsistent with, any provisions in the Agreement, the Privacy Schedule shall prevail.

1. DEFINITIONS AND INTERPRETATION

1.1. In this Privacy Schedule the following terms shall have the following meanings:

"Affiliate" means, with respect to a party, an entity that is Controlled by, Controlling, or in common Control with that party, where **"Control"** means the power to direct or cause the direction of the management and policies of an entity, whether through the ownership of voting shares, by contract, or otherwise;

"Agreement Personal Data" means any personal data or personal information (including any sensitive or special categories of data) that is transmitted, stored, or otherwise processed under or in connection with the Agreement;

"Business Day" means a day except Saturdays and Sundays and public holidays applicable in the contracting parties' jurisdiction;

"LevelBlue Group" means the LevelBlue and all its Affiliates and related/associated companies as well as joint ventures of such Affiliates and related/associated companies;

"DP Laws" means any applicable data protection and privacy laws relating to the protection of individuals with regards to the processing of personal data including but not limited to (i) the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"); (ii) the GDPR as transposed into the national laws of the United Kingdom ("**UK GDPR**"); (iii) Directive 2002/58/EC ("**ePrivacy Directive**"); (iv) the California Consumer Privacy Act of 2018 and California Privacy Rights Act of 2020 (collectively, the "**CCPA**") and any corresponding or equivalent United States state or federal laws or regulations including any amendment, update, modification to or re-enactment of such laws (together "**US Privacy Laws**"); (v) the Personal Information Protection and Electronic Documents Act ("**PIPEDA**") and any provincial privacy laws in Canada; and (vi) any corresponding or equivalent national laws or regulations including any amendment, supplement, update, modification to, or re-enactment of such laws;

"Independent DP Audit" means a data protection audit conducted by third party auditors to verify compliance with LevelBlue's processor obligations under this Privacy Schedule;

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the Agreement Personal Data;

"Restricted Transfer" means a transfer of the Agreement Personal Data between Client (or a Client Affiliate) or LevelBlue (or LevelBlue Affiliate(s)) which, in the absence of the SCCs, would be unlawful under DP Laws;

"SCCs" means (i) the standard contractual clauses set out in Commission Implementing Decision (EU) 2021/914 for the transfer of personal data to third countries pursuant to the GDPR as updated, amended, replaced, and superseded from time to time ("**EU SCCs**"); and/or (ii) the UK IDTA;

"Sell[ing]," "Sale," or "Sold" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means personal data by one business to another business or a third party for monetary or other valuable consideration;

“Sub-processor” means another processor or service provider engaged by LevelBlue as processor to carry out specific processing activities on the Agreement Personal Data; and

“UK IDTA” means either the International Data Transfer Agreement (the **“IDTA”**) or the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (the **“UK Addendum”**) issued by the UK Information Commissioner under section 119A(1) Data Protection Act 2018.

The terms **“business,” “controller,” “data subject,” “personal data,” “personal information,” “processing,” “processor,” “sensitive personal data,” “service provider,” “share,” “special categories of data,”** and **“transfer”** shall have the same meanings ascribed to them or equivalent terms under DP Laws, and references to the term **“personal data”** shall be interpreted to include any information defined as **“personal information”** or any other such similar term as defined in DP Laws.

- 1.2. Capitalized terms not defined therein shall have the meaning ascribed to them elsewhere in the Agreement.
- 1.3. Except as modified below, the terms of the Agreement shall remain in full force and effect.

2. GENERAL

- 2.1. Each party shall comply with its respective obligations under DP Laws with regards to Agreement Personal Data.
- 2.2. If the parties or their Affiliates (as applicable) enter into an Order Form or SOW, under which LevelBlue agrees to provide services to Client which:
 - (a) are listed in Appendices 1 and/or 2, then the relevant services shall be deemed applicable for the purposes of Appendices 1 and/or 2 from the date of that Order Form or SOW; or
 - (b) are not covered by Appendices 1 and/or 2, then the parties or their Affiliates (as applicable) may agree in writing to update Appendices 1 and/or 2 to insert details of the relevant services.

3. DATA PROTECTION OBLIGATIONS

- 3.1. Sections 3 to 7 shall apply only to the extent that (i) DP Laws apply to LevelBlue’s processing of Agreement Personal Data; and (ii) such laws impose or require that each of the following obligations be imposed on the parties, in light of LevelBlue’s processing of Agreement Personal Data. For the avoidance of doubt, this means that where DP Laws only impose or require certain of the following obligations, only those obligations shall apply between the parties.
- 3.2. The parties shall take all measures to comply with DP Laws.
- 3.3. Each party shall notify the other without undue delay if it is no longer able to process Agreement Personal Data in accordance with DP Laws.
- 3.4. The parties agree that the roles of the parties with respect to the processing of Agreement Personal Data will depend on the specific services provided under this Privacy Schedule as follows:
 - (a) For the services listed in Appendix 1, (**“Controller Services”**), each party acts as an independent controller or business as applicable under applicable DP Laws, with respect to the Agreement Personal Data processed in connection with the provision of such services ; and
 - (b) For the services listed in Appendix 2, (**“Processor Services”**), LevelBlue acts as a processor or service provider on behalf of Client, and Client acts as the controller or business, in respect of the Agreement Personal Data processed for the provision of the services.

- 3.5. LevelBlue and LevelBlue Affiliates may process, transfer, and disclose Agreement Personal Data as described in LevelBlue's privacy notice in particular for (i) the delivery of the Processor Services; (ii) the delivery of the Controller Services; (iii) administration of engagement and general correspondence with Client; (iv) screening of individuals associated with Client against international sanctioned parties lists; and (v) aggregation, de-identification, and, where feasible, full anonymization of Agreement Personal Data for benchmarking, market research, and data analysis purposes associated with the development of LevelBlue Group's products and services. Client acknowledges and understands that LevelBlue shall act as a controller or business of any Agreement Personal Data which is processed pursuant to this Clause 3.5 (i)-(v) and shall comply with DP Laws in respect of such processing.
- 3.6. Each party shall implement appropriate technical and organizational security measures in relation to the processing of the Agreement Personal Data under or in connection with the Agreement, which shall ensure a level of security appropriate to the risk including, as appropriate, (i) pseudonymization and encryption; (ii) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; (iii) the ability to restore the availability and access to the Agreement Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing, and evaluating the effectiveness of those measures; and (v) any other measures required by DP Laws.
- 3.7. LevelBlue shall maintain a global data governance framework which mandates technical and organizational security measures applicable to the processing of Agreement Personal Data including those relating to, without limitation, access control, data handling, malware protection, security organization, system configuration and hardening, personnel security, physical security, business continuity plans and disaster recovery, and third-party security.
- 3.8. LevelBlue shall retain the Agreement Personal Data pursuant to its corporate record retention schedules for the purposes of meeting LevelBlue's legal and regulatory obligations and enabling LevelBlue to establish, exercise, or defend legal claims.

4. **PROVISIONS APPLICABLE TO CONTROLLER SERVICES**

- 4.1. Each party agrees for its own part that, to the extent that it processes Agreement Personal Data as a separate controller:
 - (a) it will observe all applicable requirements of DP Laws and this Privacy Schedule in relation to its processing of Agreement Personal Data; and
 - (b) all Agreement Personal Data collected or sourced by it or on its behalf for processing in connection with the Agreement or which is otherwise provided or made available to the other party shall have been collected or otherwise obtained in compliance with DP Laws, and may be processed, disclosed, and transferred as described in or in connection with the Agreement.
- 4.2. The parties will work together in good faith to ensure the information prescribed by DP Laws is made available to relevant data subjects, including where necessary the Client's provision of such information to data subjects on LevelBlue's behalf.
- 4.3. If either party receives any complaint, notice, or communication from a supervisory authority which relates to the other party's (i) processing of the Agreement Personal Data; or (ii) potential failure to comply with DP Laws in respect of the Agreement Personal Data, that party shall direct the supervisory authority to the other party.
- 4.4. If a data subject makes a written request to a party to exercise any of their rights in relation to the Agreement Personal Data that concerns processing of the other party, that party shall direct the data subject to that other party. Where such a request relates to the processing of Agreement Personal

Data by LevelBlue as processor on behalf of the Client, the obligations set out in Clause 5.7 below shall apply.

- 4.5. If either party becomes aware of a Personal Data Breach that requires notification to a supervisory authority, it shall notify the other party without undue delay, and each party shall cooperate with the other, to the extent reasonably requested, in relation to any notifications to supervisory authorities and/or to affected data subjects.

5. PROVISIONS APPLICABLE TO PROCESSOR SERVICES

- 5.1. LevelBlue shall process the Agreement Personal Data only in accordance with Client's instructions as set out in the Agreement, or from time to time by written agreement of the parties, including as to the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, in each case, which are more specifically set out in Appendix 2, unless required by law to act without such instructions, in which case LevelBlue shall, to the extent legally permitted, promptly inform Client upon becoming aware of such legal requirement.
- 5.2. LevelBlue shall not retain, use, or disclose Agreement Personal Data outside of the Agreement between LevelBlue and Client.
- 5.3. LevelBlue shall permit Client to take any reasonable and appropriate steps to stop and remediate any actual or suspected unauthorized use of Agreement Personal Data.
- 5.4. If LevelBlue considers that any instructions from Client relating to processing of Agreement Personal Data may put LevelBlue in breach of DP Laws, LevelBlue will inform Client and will be entitled not to carry out that processing and will not be in breach of the Agreement or otherwise liable to Client as a result of its failure to carry out that processing.
- 5.5. LevelBlue shall ensure that any personnel, agents, and/or contractors who process the Agreement Personal Data are subject to appropriate contractual or statutory obligations of confidentiality.
- 5.6. LevelBlue shall implement appropriate technical and organizational security measures as described in Clauses 3.6 and 3.7.
- 5.7. In relation to the Agreement Personal Data, taking into account the nature of the processing activities and the information available to LevelBlue, LevelBlue shall, upon written request from Client, provide reasonable assistance to Client in ensuring compliance with Client's obligations under DP Laws with respect to:
 - (a) responding to requests by data subjects in relation to their rights under DP Laws;
 - (b) the performance of data protection impact assessments or other risk assessments required by DP Laws, and mandatory prior consultation with a supervisory authority; and
 - (c) without prejudice to Clause 5.7(a), where LevelBlue receives a request directly from a data subject exercising their rights under DP Laws in relation to the Agreement Personal Data, LevelBlue shall forward the request to the Client promptly, and will provide reasonable assistance to Client to enable Client to respond to that request.
- 5.8. At Client's choice and written request, LevelBlue shall delete or return the Agreement Personal Data to Client at the end of the term of the Agreement and delete any copies of the Agreement Personal Data unless it is required to retain such copies pursuant to applicable law.
- 5.9. LevelBlue will, upon becoming aware, notify Client without undue delay of any Personal Data Breach materially impacting on Client and will provide reasonable assistance to Client in response to such Personal Data Breach, to enable Client to meet its obligations under DP Laws as regards the notification to supervisory authorities and/or affected data subjects. For these purposes LevelBlue will provide Client all details as required by applicable DP Laws. The parties agree that such details may be provided to Client in phases and to the extent these are known to LevelBlue.

- 5.10. LevelBlue is hereby generally authorized by Client to engage any Sub-processor, provided that LevelBlue shall (i) ensure in each case that the Sub-processor is bound by data protection obligations that are substantially the same as those contained in the Agreement; (ii) subject to the terms of the Agreement (including but not limited to any limitations on liability agreed therein), remain fully liable to Client for the performance of that Sub-processor's obligations; and (iii) maintain a list of all such Sub-processors.
- 5.11. LevelBlue shall maintain a list of Sub-processors and make such list available to Client via a designated notification mechanism. Client shall be subscribed to such notification mechanism in order to receive updates regarding Sub-processor changes. LevelBlue shall provide notice of any addition or replacement of a Sub-processor through such notification mechanism. Client shall have fifteen (15) days from the date the notice is made available to object to the change by providing written notice to LevelBlue stating the reasonable and documented grounds for such objection. If Client does not object within the fifteen (15) day period, the Sub-processor change shall be deemed approved. In the event Client raises a timely objection, the parties shall work in good faith to resolve the objection. If the parties are unable to reach a commercially reasonable resolution and the objection is reasonable founded on data protection grounds, Client may terminate the affects services upon written notice to LevelBlue.
- 5.12. Client agrees that LevelBlue may continue to use those Sub-processors already engaged by LevelBlue or any LevelBlue Affiliates as at the date of the Agreement provided that in each case as practicable LevelBlue meets the obligations set out in Clause 5.10.
- 5.13. LevelBlue shall, on reasonable written request, (i) make available to Client information that is reasonably necessary to demonstrate compliance with LevelBlue's processor obligations. To the extent reasonably possible, LevelBlue may satisfy such obligation by providing summaries of relevant audit reports, certifications, or other documentation demonstrating LevelBlue's compliance with recognized security and data protection standards. If the information provided by LevelBlue does not reasonably demonstrate such compliance, Client may request additional information in the form of a written questionnaire regarding LevelBlue's data protection and security practices. Only where the foregoing measures are not reasonably sufficient to demonstrate compliance, and no more than once per twelve (12) month period, Client may request an audit, but in each case only if such information and audits are in relation to the Agreement Personal Data processed pursuant to the Agreement. Any such audit shall, (1) be limited to the processing of Agreement Personal Data under the Agreement, (2) be conducted during normal business hours with reasonable advance written notice, (3) be subject to appropriate confidentiality obligations, (4) not unreasonably interfere with LevelBlue's business operations or compromise the security or confidentiality of other customers' data; and (5) be conducted by an independent third party auditor at Client expense and mutually agreed by the parties. LevelBlue shall notify Client in writing if it believes in good faith that the exercise of rights under this Clause 5.13 would infringe the relevant DP Laws.
- 5.14. Client agrees to exercise its rights for information, audits, and inspections under Clause 5.13 above by permitting LevelBlue to carry out an Independent DP Audit, pursuant to which LevelBlue agrees to provide Client, upon written request, with a confidential audit report to enable Client to reasonably verify LevelBlue's compliance with its processor obligations under the Privacy Schedule.
- 5.15. Notwithstanding Clause 5.13 and Clause 5.14, in the event of a Personal Data Breach, Client shall be entitled on ten (10) Business Days' prior notice to LevelBlue, during normal business hours, causing minimal disruption, and subject to LevelBlue's obligations of confidentiality to carry out an audit of LevelBlue to reasonably verify LevelBlue's compliance with its processor obligations, subject to the conditions of Clause 5.13.

- 5.16. Should any audit report identify material non-compliance with LevelBlue's processor obligations, the parties shall work together in good faith to mutually agree to steps to reasonably address such non-compliance.
- 5.17. LevelBlue shall provide to Client information to demonstrate LevelBlue's technical and organizational measures used by LevelBlue to ensure the security of Agreement Personal Data to ensure compliance with DP Laws.
- 5.18. The parties acknowledge that Agreement Personal Data may be transferred or otherwise processed or transferred outside of its country of origin ("**International Transfers**") by LevelBlue including by any Sub-processors engaged in accordance with the Agreement, provided that such International Transfers are made in compliance with DP Laws, including, if applicable, by adoption of SCCs, or such other international transfer mechanism that effectively complies with DP Laws.
- 5.19. With respect to Agreement Personal Data, LevelBlue shall not Sell or share such data for cross-context behavioral advertising purposes.

6. PROVISIONS APPLICABLE TO RESTRICTED TRANSFERS

- 6.1. With respect to Restricted Transfers the SCCs are hereby incorporated into this Agreement by reference and will come into effect upon commencement of any such Restricted Transfer, and the following terms shall apply. In each case, the data exporter is the party or its Affiliates (as applicable) disclosing the Agreement Personal Data and the data importer is the party or its Affiliates (as applicable) receiving the Agreement Personal Data:
 - (a) where a Restricted Transfer is subject to the GDPR the following terms shall apply:
 - (i) Annex IA of the EU SCCs will be populated with the details of the parties set out in the Agreement, Annex IB of the EU SCCs will be populated with the description of processing of personal data set out in the Appendices to this Privacy Schedule; and
 - (ii) For the purposes of Modules 1, 2 and 3 of the EU SCCs: clause 7 and the optional language in clause 11(a) shall not apply, for the purposes of clause 9, the parties select Option 2 (general authorization) for which notification shall be within a commercially reasonable time period, the supervisory authority for the purposes of clause 13(a) shall be determined by the place of establishment of the data exporter, the governing law and choice of forum and jurisdiction stipulated in the Agreement shall apply to the extent that it is the law and the courts of an EU member state otherwise it shall be those of the Republic of Ireland, and the technical and organizational security measures set out in Clauses 3.6 and 3.7 shall apply. The frequency of the transfer shall be continuous, as necessary to deliver the Controller and Processor Services, and retention shall be determined by the Client, except where LevelBlue is required by applicable laws to retain Agreement Personal Data in accordance with LevelBlue's corporate record retention schedules and policies.
 - (b) where a Restricted Transfer is subject to the GDPR and UK GDPR the following terms with respect to the UK Addendum shall, in addition to Clause 6.1(a) above, also apply:
 - (i) the EU SCCs shall be read in accordance with, and deemed amended by, the provisions of Part 2 (Mandatory Clauses) of the UK Addendum; and
 - (ii) the parties confirm that the information required for the purposes of Part 1 (Tables) of the UK Addendum is set out in the Agreement.
 - (c) where a Restricted Transfer is subject to the UK GDPR the parties confirm that the information required for the purposes of Part 1 (Tables), Part 2 (Extra Protection Clauses), and Part 3 (Commercial Clauses) of the IDTA is set out in the Agreement and the

Appendices to this Privacy Schedule and the organizational and technical measures described in Clauses 3.6 and 3.7 shall apply.

- 6.2. For the avoidance of doubt (and without prejudice to third party rights for data subjects under the SCCs) the parties hereby submit to the limitations stipulated in the Agreement with respect to their respective liability towards one another under the SCCs.
- 6.3. To the extent that there is any conflict or inconsistency between the terms of the SCCs and the terms of the Agreement, the terms of the SCCs shall take precedence.
- 6.4. If, and to the extent that, the European Commission or the United Kingdom issues any amendment to, or replacement of, the EU SCCs or the UK IDTA pursuant to Article 46(5) or Article 46 of the GDPR or UK GDPR, the parties agree in good faith to take such additional steps as necessary to ensure that such replacement terms are implemented across all transfers.
- 6.5. If, at any time, a supervisory authority or a court with competent jurisdiction over a party mandates that transfers from controllers in the European Economic Area (“**EEA**”) or the United Kingdom to controllers or processors established outside the EEA or the United Kingdom must be subject to specific additional safeguards (including but not limited to specific technical and organizational measures), the parties shall work together in good faith to implement such safeguards and ensure that any transfer of Agreement Personal Data is conducted with the benefit of such additional safeguards.

7. **PROVISIONS APPLICABLE TO BUSINESS OR SERVICE PROVIDER**

- 7.1. To the extent LevelBlue is providing Controller Services pursuant to the Agreement, Client has contractually engaged LevelBlue to perform the Controller Services in support of one or more specified purposes. In order for LevelBlue to provide the Controller Services to Client and to perform its obligations under the Agreement, Client must provide, direct others to provide, or otherwise make available (collectively “**provide**”) to LevelBlue certain data, including Agreement Personal Data (“**Relevant Data**”). Client agrees to provide to LevelBlue the Relevant Data that is necessary for LevelBlue’s performance of its obligations under the Agreement, and to only provide such personal data as is reasonably necessary to the performance of the Controller Services. The parties agree that (i) LevelBlue is not able to perform its obligations to Client under the Agreement unless Client provides the Relevant Data; (ii) the Relevant Data is necessary to the performance of the Controller Services in support of the Agreement’s specified purposes; and (iii) the Agreement Personal Data is not provided to LevelBlue in exchange for any monetary or other valuable consideration from LevelBlue to Client. LevelBlue does not Sell any personal information as part of the Controller Services provided under the Agreement.
- 7.2. To the extent that LevelBlue provides Processor Services pursuant to the Agreement, the parties intend and agree that Client is a business and LevelBlue is a service provider for the purposes of and as defined by the CCPA in respect of the Agreement Personal Data processed pursuant to the Processor Services which LevelBlue provides to Client under the Agreement. LevelBlue shall only retain, use, or disclose Agreement Personal Data under this Privacy Schedule for the specific purpose of performing the services under the Agreement and this Privacy Schedule. Without limiting the generality of the foregoing, LevelBlue is prohibited from:
 - (a) Selling or sharing Agreement Personal Data;
 - (b) retaining, using, or disclosing any Agreement Personal Data for any purpose other than for the business purposes specified in the Agreement;
 - (c) retaining, using, disclosing, or otherwise processing Agreement Personal Data outside of the direct business relationship between Client and LevelBlue; and

- (d) combining Agreement Personal Data received from or on behalf of Client with personal data that it receives from, or on behalf of, another person or persons, or collects from its own interaction with a consumer, except where both (i) expressly required to perform the services; and (ii) permitted by DP Laws.

LevelBlue hereby certifies that it understands the restrictions set forth in this Clause 7.2 and will comply with them.

Appendix 1: Controller Services

| Description of processing | | |
|--|--|---|
| Where applicable, for the purposes of Annex 1 to Module 1 of the EU SCCs, Annex B of the Controller SCCs and/or any IDTA, the data exporter(s) is the party disclosing the Agreement Personal Data and the data importer(s) is the party receiving the Agreement Personal Data. The Agreement Personal Data is processed for the purposes of providing the Controller Services listed below and is processed for the duration of the Agreement. Processing operations may be set out more specifically in the Agreement and/or any applicable Order Form or SOW. | | |
| Service | Type of Personal Data | Categories of Data Subject |
| The provision of engagement services which include forensic accounting, investigations, intelligence, Products | <ul style="list-style-type: none"> Personal details Financial details Criminal offense details Family, lifestyle & social circumstances Employment details Business related activities Personal data may also concern the following special categories of data: data concerning health, data concerning a natural person's sex life or sexual orientation | <ul style="list-style-type: none"> Client's employees and, where applicable, employees of Client's client Client's users and, where applicable, users of Client's client Suppliers/contractors of Client and, where applicable, Client's client Client's counsel and Client's counsel's users Members of the public Relations of employees (family members, emergency contacts) |

Appendix 2: Processor Services

| Description of processing | | |
|--|--|---|
| Where applicable, for the purposes of Annex 1 to Module 2 of the EU SCCs and Appendix 1 of the Processor SCCs and/or any IDTA, the data exporter(s) is the party disclosing the Agreement Personal Data and the data importer(s) is the party receiving the Agreement Personal Data. The Agreement Personal Data is processed for the purposes of providing the Processor Services listed below and is processed for the duration of the Agreement. Processing operations may be set out more specifically in the Agreement and/or any applicable Order Form or SOW. | | |
| Service | Type of Personal Data | Categories of Data Subject |
| The provision of engagement services which include security advisory and testing, digital forensics, incident response, and intellectual property , or services that may be performed by AlertLogic, Cybereason, or Trustwave entities . | <ul style="list-style-type: none"> Personal details Financial details Family, lifestyle & social circumstances Employment details Business related activities Personal data may also concern the following special categories of data: data concerning health, data concerning a natural person's sex life or sexual orientation | <ul style="list-style-type: none"> Client's employees and, where applicable, employees of Client's client Client's users and, where applicable, users of Client's client Suppliers/contractors of Client and, where applicable, Client's client Client's counsel and Client's counsel's users Members of the public Relations of employees (family members, emergency contacts) |

In the event a service is not listed in Appendix 1 or Appendix 2, the parties will determine the applicable roles under applicable DP Laws based on the nature of the processing activities performed.