Expel, Inc.
Data Processing Agreement

This Data Processing Agreement (this "**DPA**") is effective as of (the "**DPA Effective Date**") by and between or its applicable Affiliates ("**Customer**") and **Expel, Inc.**, a Delaware corporation or its applicable Affiliates ("**Vendor**" or "**Expel**"). The Vendor provides certain software, hardware and/or services (collectively "**Services**") to Customer under various agreements between Customer and Vendor (collectively the "**Vendor Agreement**").

Customer Name:	**Vendor: Expel, Inc.**
Addresses for notices under this DPA: Address: Email**:** cc:	**Addresses for notices under this DPA:** Address: 12950 Worldgate Dr., Suite 200 Herndon, VA 20170 Email: privacy@expel.com
Signature:	**Signature:**
Name:	**Name:** Peter Katz
Title:	**Title:** VP, General Counsel
Date Signed:	**Date Signed:**

By signing this DPA, each party acknowledges that it has read and understood the terms of this DPA, as set forth below, and agrees to be bound by them.

1. DEFINITIONS

1.1 **Affiliate**(**s**) means an entity that directly or indirectly Controls, is Controlled by or is under common Control with a Party to this DPA. "Control" means an ownership, voting or similar interest representing fifty percent (50%) or more of the total interests then outstanding of the entity in question. The term "Controlled" will be construed accordingly.

1.2 **Applicable Privacy Laws** means any data protection laws or regulations applicable to the processing (including transfer) of Customer Data in a specific jurisdiction (examples of which may include the EU Regulation 2016/679 (the "**EU GDPR**"), the UK Data Protection Act 2018 which implemented the UK General Data Protection Regulation (the "**UK GDPR**"), the California Consumer Privacy Act of 2018 (the "**CCPA**"), and the California Privacy Rights Act (the "**CPRA**") in each case, to the extent in force, and as updated, amended or replaced from time to time.

1.3 **Customer Data** means any data which is (i) defined as "Personal Data" "Personal Information" "Personally Identifiable Information" or any substantially similar term under Applicable Privacy Laws and (ii) processed on behalf of Customer by Vendor (including Personnel or Sub-Processors) in connection with the Vendor Agreement.

1.4 **Data Exporter or Data Controller** means the Customer that sends Customer Data to Vendor so it can be processed in accordance with the Vendor Agreement and this DPA.

1.5 **Data Importer or Data Processor** means the Vendor that receives Customer Data from Customer so it can be processed on behalf of Customer in accordance with the Vendor Agreement and this DPA.

1.6 **Personnel** means any employees, Sub-Processors or other personnel of Vendor who are authorized to process Customer Data under the authority of Vendor.

1.7 **Security Incident** means any reasonably suspected or actual accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Data being processed by Vendor. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Customer Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks or other network attacks on firewalls or networked systems.

1.8 **Standard Contractual Clauses ("SCCs")** means, as applicable to a particular transfer, one of the following:

(1) **EU/EEA SCCs** are the contractual clauses that the General Data Protection Regulation ("**GDPR**") states, which ensure appropriate data protection safeguards that can be used as a ground for data transfers from the EU to third countries. This includes SCCs that have been "pre-approved" by the European Commission. The EU/EEA SCCs encompass the updates made by the EU Commission on 4 June 2021, the Commission issued modernised standard contractual clauses under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR).

(2) **UK Standard Contractual Clauses ("UK SCCs")** means the UK Addendum to the EEA SCCs adopted pursuant to or permitted under Article 46 of the UK GDPR.

(3) **UK International Data Transfer Agreement** ("UK IDTA") - adopted pursuant to or permitted under Article 46 of the UK GDPR.

1.9 **Sub-Processor(s)** means any subcontractor (including any Affiliates of the Vendor) appointed by the Vendor, and approved by Customer, in accordance with Section 3 of this DPA, to process Customer Data.

1.10 The following terms (and any substantially similar terms under Applicable Privacy Laws) shall have the meanings and otherwise be interpreted in accordance with Applicable Privacy Laws: Data Controller, Data Processor, Data Subject, Data Subject Request, Personal Data, process(ing) and transfer.

2. DPA SCOPE AND PROCESSING BY VENDOR

2.1 **Scope of DPA.** The parties agree that this DPA shall govern the processing of any Customer Data by Vendor (including by Vendor Personnel) in connection with the Vendor Agreement(s). The details of processing under this DPA are set forth in **Exhibit 1 – Details of Processing**. If relevant to the jurisdiction where Vendor's Services are contracted or provided, Vendor shall be considered a Data Processor under the EU GDPR and UK GDPR and/or a Service Provider under the CCPA, and may be subject to similar designations in other jurisdictions. This DPA shall be effective as of the DPA Effective Date and shall remain in effect for the duration of the applicable Vendor Agreement.

2.2 **Compliance with law.** The Vendor warrants that, in relation to the Customer Data, Vendor shall (and will ensure that its Personnel shall) comply with all Applicable Privacy Laws.

2.3 **Instructions.** The Vendor shall process the Customer Data solely as necessary to provide the Services to Customer and at all times in accordance with Customer's documented instructions (including with regard to transfers of Customer Data to a third country or an international organisation), as provided in this DPA or as provided thereafter, in writing, by an authorized representative of Customer (collectively "**Instructions**"). Vendor shall immediately notify Customer if it believes that an Instruction violates Applicable Privacy Laws.

2.4 **Purpose limitation** Vendor may not retain, use or disclose the Customer Data (and may not permit its Personnel to retain, use or disclose the Customer Data) for any purpose other than for the specific business purpose of performing the Services in the Vendor Agreement for Customer.

3. SUB-PROCESSING AND PERSONNEL

3.1 Customer consents to Vendor's use of the Sub-Processors as set forth at https://www.expel.com/notices and the Expel Trust Center (https://security.expel.com).

3.2 If the Vendor wishes to replace or appoint any new Sub-Processor, Vendor shall provide at least fourteen (14) days prior written notice to Customer of the Sub-Processor change and associated details of processing, except that if Vendor reasonably believes engaging a new Sub-Processor on an expedited basis is necessary to protect the confidentiality, integrity or availability of the Customer Data or avoid a material disruption to the Services, Vendor will give such notice as soon as reasonably practicable. Updates to the Sub-Processor List will be posted in the Expel Trust Center and a notification will be sent via email to [customer to provide email address]. The Customer will be provided with fourteen (14) days to review ('**Review Period**'). The parties agree that non-response by the Customer during the Review Period will be taken as the Customer's approval of that Proposed Sub-Processor Update. If Customer objects to a Sub-Processor proposed under this Section 3.2 on good faith data processing grounds, Vendor shall provide Customer with reasonable alternative(s), if any, to such engagement, including without limitation, modification to the Services. If Vendor cannot provide any such alternative(s), or if Customer, acting reasonably, does not agree to any such alternative(s), Customer may terminate the Vendor Agreement and this DPA and Vendor shall provide Customer with a pro-rata refund for all fees paid by Customer for Services not yet received.

3.3 With respect to all Sub-Processors authorized under Section 3.1 or 3.2:

(1) Vendor is responsible and liable to Customer for any processing by a Sub-Processor in breach of this DPA or Applicable Privacy Law. Where any provision of this DPA places an obligation on the Vendor, that obligation shall be construed as an obligation on the Vendor to ensure that all its Personnel and its Sub-Processors (and its Sub-Processors' personnel) comply with such obligation. In particular, Vendor shall ensure that such Sub-Processor shall only process Customer Data in accordance with the Instructions and as strictly necessary to provide the Services to Customer.

(2) Prior to such Sub-Processor processing the Customer Data, Vendor shall enter into a written agreement with each Sub-Processor which (a) requires the Sub-Processor to process the Customer Data as required by Applicable Privacy Laws; and (b) is at a minimum, as protective of Customer Data as this DPA.

3.4 Vendor shall limit access to, and processing of, Customer Data to those Personnel who are necessary to provide the Services and shall ensure that any Personnel who are authorized by Vendor to process Customer Data are under a binding obligation of confidentiality with respect to the processing of the Customer Data.

4. INTERNATIONAL TRANSFERS

4.1 **Permitted Regions.** Absent the written consent of Customer, Vendor shall not process Customer Data in, or transfer Customer Data to, any region other than a "**Permitted Region**", as noted in **the Sub-Processor List** noted in Section 3.1.

4.2 **Adequate Level of Protection.** Vendor will at all times provide an adequate level of protection for the Customer Data, wherever transferred or processed, in accordance with the requirements of Applicable Privacy and Data Protection Laws.

4.3 **International Transfers involving Europe.** Where Customer Data is transferred by Vendor from the European Union, the European Economic Area (EEA) and/or their member states, Switzerland, and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Applicable Privacy and Data Protection Laws and Regulations, to the extent such transfers are subject to such Data Protection Laws and Regulations: the parties agree that the EU/EEA SCCs for Processors (also known as "**Model Clauses**") as set forth at https://www.expel.com/notices shall apply**,** with Customer as "data exporter" and Vendor as "data importer" (as defined in the Model Clauses).

(1) Application of the EU SCCs: Where Vendor Processes Customer Personal Data subject to the EU GDPR in a country outside the Permitted Territories, the parties enter into and agree to be bound by the provisions of the EU Processor to Processor SCCs approved with Commission Implementing Decision (EU) 2021/914 of June 4, 2021 on SCCs for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("EU SCCs"), with Customer as "data exporter" and Supplier as "data importer." In addition:

(a) Module 1 (Controller to Controller) will apply where Customer is a Controller of Personal Data and Vendor is a Controller of Personal Data;

(b) Module 2 (Controller to Processor) will apply where Customer is a Controller of Personal Data and Vendor is a Processor of Personal Data;

(i) For each module, where applicable:

1. in Clause 7, the option docking clause will not apply.
2. in Clause 9, Option 2 will apply, and the time period for prior notice of a sub-processor will be as set forth in Section 3 of the DPA.
3. Clause 11, the optional language is excluded.
4. In Clause 17, the governing law shall be the law of Ireland;
5. In Clause 18, disputes shall be resolved in the courts of Ireland;
6. The competent supervisory authority shall be the Irish Data Protection Commission; and
7. The remaining information required by the Annexes to the EU/EEA SCCs is set forth in the Exhibits to this DPA.

(2) For transfers from Switzerland:

(a) The supervisory authority with respect to such Personal Data is the Swiss Federal Data Protection and Information Commissioner.

(b) References to a "Member State" shall be interpreted to refer to Switzerland.

(c) Data subjects located in Switzerland shall be able to enforce their rights in Switzerland.

(d) References to the EU GDPR shall be understood to refer to the Swiss Federal Act on Data Protection (as amended or replaced).

(e) Clause 17 (Governing Law)(Option 1), the law of Switzerland will apply.

(f) Clause 18(b), disputes will be resolved in the courts of Switzerland.

(g) References to the "competent supervisory authority" and "competent courts" shall be interpreted as references to the Swiss Federal Data Protection and Information Commissioner and competent courts in Switzerland, unless the EU SCCs, implemented as described above, cannot be used to lawfully transfer such Personal Data in compliance with the Swiss DPA in which case the Swiss SCCS shall instead be incorporated by reference and form an integral part of this DPA and shall apply to such transfers. Where this is the case, the relevant Annexes or Appendices of the Swiss SCCs shall be populated using the information contained in Exhibits 1 and 2 of this DPA (as applicable);

(3) Application of the UK SCCs. For Personal Data transfers from the EEA or Switzerland and the UK, the EU/EEA SCCs will apply as noted in this Section 4, and the UK Addendum to the EU/EEA SCCs will apply to the Personal Data being transferred from the UK.

(4) Application of the UK International Data Transfer Agreement. For Personal Data transfers from the UK that do not also involve Personal Data being transferred from the EEA or Switzerland ("**Transferred Data**"), then the UK IDTA will apply as follows:

(a) Part one: Tables

(i) Table 1: Parties and signature: This Table shall be deemed completed with the information in Exhibit 1 of this DPA and the signatures to the DPA.

(ii) Table 2: Transfer Details

1. UK country's law that governs the IDTA: England and Wales
2. Place for legal claims to be made: England and Wales
3. The status of the importer: Importer is the Exporter's Processor or Sub-Processor
4. Whether the UK GDPR applies to the Importer: UK GDPR applies to the Importer's Processing of the Transferred Data
5. Linked Agreements: The Agreement, Service Orders, and this DPA.

6. Term: The Importer may Process the Transferred Data for the following time period: the period for which the Linked Agreement is in force.

7. Ending the IDTA before the end of the term: the Parties cannot end the IDTA before the end of the Term unless there is a breach of the IDTA.

8. Can the Importer make further transfers of the Transferred Data? The Importer MAY transfer on the Transferred Data to another organisation or person (who is a different legal entity) in accordance with IDTA Section 16.1 (Transferring on the Transferred Data).

9. Specific restrictions when the Importer may transfer on the Transferred Data: The Importer MAY ONLY forward the Transferred Data in accordance with IDTA Section 16.1 pursuant to the terms of Section 3 of the DPA.

10. Review Dates: The Parties must review the Security Requirements at least once: each time there is a change to Transferred Data, Purposes, Importer Information, TRA, or risk assessment.

(iii) Table 3: Transferred Data

1. Transferred Data: This Table shall be deemed completed with the information in Exhibit 1 of this DPA.

(iv) Table 4: Security Requirements: This Table shall be deemed completed with the information in Exhibit 2 of this DPA.

(v) Part two: Extra Protection Clauses: Intentionally omitted

(vi) Part three: Commercial Clauses: Intentionally omitted

(vii) Part four: Mandatory Clauses: no modifications

(5) It is not the intention of either party to contradict or restrict any of the provisions set forth in the SCCs and, accordingly, if and to the extent the SCCs conflict with any provision of the Agreement (including this DPA) the SCCs shall prevail to the extent of such conflict;

4.4 In the event International Transfers occur from a country not listed in this clause 4, the Vendor shall work in good faith with the Customer to ensure appropriate safeguards both from a legal and security perspective are applied and meet the requirements of data transfers pursuant to Applicable Privacy and Data Protection Laws.

4.5 The Vendor shall comply with its obligations therein and such Model Clauses will form an integral part of this DPA. Where and to the extent there is any conflict between this DPA, the Vendor Agreement(s), and the Model Clauses, the Model Clauses will prevail in all cases. If and to the extent that the Model Clauses apply, signatures of assent of Customer and Vendor to this DPA will be deemed signatures to the Model Clauses.

5. SECURITY AND SECURITY INCIDENTS

5.1 **Confidentiality.** Vendor shall ensure that all Personnel are subject to a strict duty of confidentiality (whether a contractual or statutory duty) and that they process the Personal Data only for the purpose of delivering the Services to Customer under the Vendor Agreement. Vendor shall not disclose any Customer Data (including any disclosure to Personnel) other than at the written request of Customer or as expressly permitted in this DPA or the Vendor Agreement. If Vendor receives a subpoena, court order, warrant or other legal demand from a third party (including law enforcement or other public or judicial authorities) seeking the disclosure of Customer Data, Vendor shall, legally permitting, immediately notify Customer in writing of such request prior to disclosing such Customer Data and reasonably cooperate with Customer if it wishes to limit, challenge or protect against such disclosure, to the extent permitted by applicable laws.

5.2 **Data Retention.** Upon Customer's written request or upon termination or expiration of the Vendor Agreement, Vendor shall either return to Customer, or irretrievably delete, all Customer Data (including all copies of such data) in its possession or control (including all Customer Data processed by its Personnel under this DPA). This requirement shall not apply to the extent that Vendor is required by any applicable law to retain some or all of the Personal Data, in which event Vendor shall isolate and protect the Personal Data from any further processing except to the extent required by such law.

5.3 **Technical and Organizational Security Measures.** Vendor represents and warrants that is has implemented and will maintain appropriate technical and organizational security measures to protect Customer Data from Security Incidents and to preserve the security and confidentiality of the Customer Data and to comply with Applicable Privacy Laws, such measures shall include, but not be limited to, those security measures set forth in **Exhibit 2 - Technical and Organizational Security Measures.**

5.4 **Security Incident Initial Notice.** Vendor shall, without undue delay (and in any event within seventy-two (72) hours) after discovering a Security Incident, notify Customer of the Security Incident and, on a continuously updated basis when requested by Customer, provide written details of the Security Incident, including the type of data affected and the identity of the affected person(s) as soon as such information becomes suspected, known or available to Vendor.

5.5 **Security Incident Ongoing Response.** In the event of a Security Incident, Vendor shall continue to provide timely information and cooperation as Customer may require to fulfill Customer's data breach reporting requirements, including obligations under Applicable Privacy Laws and to Customer's customers; and shall take such measures and actions as are appropriate to remedy or mitigate the effects of the Security Incident and shall keep Customer up-to-date about all developments in connection with the Security Incident.

5.6 **Disclosure of Security Incident.** Insofar as it relates to or may be associated with Customer or any Customer Data, the content and provision of any notification, public/regulatory communication or press release concerning the Security Incident shall be solely at Customer's discretion, except as otherwise required by applicable laws.

6. COOPERATION AND AUDITS

6.1 **Subject Request Cooperation.** Vendor shall provide Customer with reasonable cooperation to enable Customer to respond to and fulfil any requests, complaints or other communications from Data Subjects and regulatory or judicial bodies relating to the processing of Customer Data under the Vendor Agreement, including requests from Data Subjects seeking to exercise their rights under Applicable Privacy Laws. In the event that any such request, complaint or communication is made directly to Vendor, Vendor shall promptly pass this on to Customer and shall not respond to such communication without Customer's express authorization (unless otherwise required by law, including to verify Vendor's obligations with respect to such request).

6.2 **Compliance with Law Cooperation**. In accordance with Applicable Privacy Laws, Vendor will provide Customer (or Customer's third-party Data Controller, as applicable) with reasonable cooperation and assistance to comply with its obligations under Applicable Privacy Laws, including Articles 32 through 36 of the GDPR. In particular, Vendor will promptly notify Customer if it believes that its processing of Customer Data is likely to result in a high risk to the privacy rights of Data Subjects, and upon reasonable request, will assist Customer (or Customer's third-party Data Controller, as applicable) to carry out data protection impact assessments or consult with applicable data protection authorities.

6.3 **Information Security.** Vendor shall maintain records in accordance with its SOC-2 framework and statements and ISO 27001, or similar Information Security Management System ("**ISMS**") standards. Upon request, Vendor shall provide copies of relevant external ISMS certifications, audit report summaries and/or other documentation reasonably required by Customer to verify Vendor's compliance with this DPA.

6.4 **Records and Audits.** The Vendor shall make available to Customer all information necessary to demonstrate compliance with the obligations laid down by Applicable Privacy Laws and allow for and contribute to audits (at least one (1) time per year, including inspections conducted by Customer or a third-party auditor selected by Customer. In lieu of an audit, the Customer can provide the Vendor with a security questionnaire and/or the Customer may access the Vendor's online compliance library to access security and privacy audit related documentation. .While it is the parties' intention to ordinarily rely on Vendor's obligations set forth in Section 6.3 to verify Vendor's compliance with this DPA, Customer (or its appointed representatives) may carry out an inspection of the Vendor's data processing operations and facilities during normal business hours and subject to reasonable prior notice where Customer considers it necessary or appropriate (for example, without limitation, where Customer has reasonable concerns about Vendor's data protection compliance, following a Security Incident or following instruction from a data protection authority). Additional audits beyond one (1) per year may be allowed by the Vendor as long as they are requested by a regulatory authority to assess the Vendor's compliance in accordance with this DPA and following a Security Incident affecting Customer's data.

7. Additional Provisions for California Personal Information

7.1 **Scope of Section 7.** This Section 7 (Additional Provisions for California Personal Information) shall apply only with respect to California Personal Information.

(1) **Roles of the Parties.** When Processing California Personal Information in accordance with Customer's Instructions, the parties acknowledge and agree that Customer is a Business and Vendor is a Service Provider for the purposes of the CCPA.

7.2 **Responsibilities.** The parties agree that Vendor will process California Personal Information as a Service Provider strictly for the purpose of performing its obligations under the Vendor Agreement (the "**Business Purpose**"). The Parties agree that Vendor shall not: (a) Sell California Personal Information (as defined in the CCPA); (b) retain, use, or disclose California Personal Information for a commercial purpose other than for the Business Purpose or as otherwise permitted by the CCPA; or (c) retain, use, or disclose California Personal Information outside of the direct business relationship between Customer and Vendor**.** Vendor certifies that it understands and will comply with the restrictions set out in Section 7.2 (Responsibilities).

8. MISCELLANEOUS

8.1 For the avoidance of doubt, any claim or remedies that Customer may have against Vendor (including Vendor's Personnel and its respective personnel or sub-processors) arising under or in connection with this DPA, including: (i) for breach of this DPA; (ii) as a result of fines (administrative, regulatory or otherwise) imposed upon Customer in connection with the subject matter of this DPA; or (iii) under Applicable Privacy Laws, including any claims relating to damages paid to a Data Subject, except to the extent prohibited by Applicable Privacy Laws, shall be subject to any exclusion of damages or limitation of liability provisions (including any agreed upon aggregate financial caps) that may apply under the Vendor Agreement.

8.2 The obligations placed upon the Vendor under this DPA shall survive so long as Vendor and/or its Personnel process Personal Data on behalf of Customer in connection with the Vendor Agreement.

8.3 Except as set out in this DPA, the provisions of the Vendor Agreement shall remain unchanged and shall continue in force. In the event of any conflict between this DPA and any provisions set out in any Vendor Agreements, the parties agree that the terms of this DPA shall prevail.

8.4 No variation of this DPA shall be valid unless it is in writing (which excludes email) and signed by or on behalf of each of the parties by their respective authorised representatives.

8.5 No single or partial exercise, or failure or delay in exercising any right, power or remedy by any party shall constitute a waiver by that party of, or impair or preclude any further exercise of, that or any right, power or remedy arising under this DPA or otherwise.

8.6 Excluding conflict of laws rules, this DPA shall be governed by and construed under the laws of the State of Delaware, U.S.A. All disputes arising out of or in relation to this DPA shall be submitted to the exclusive jurisdiction of the courts of New Castle County, Delaware. Nothing in this Section shall restrict Customer's right to bring an action against Vendor in the jurisdiction where Vendor's place of business is located.

Exhibit 1

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

Name:

Address:

Contact person's name, position and contact details:

Activities relevant to the data transferred under these Clauses: Managed Detection and Response Services - provision of the Services by Data Importer on behalf of the Data Exporter as further described in the Vendor Agreement.

Role (controller/processor): **Controller**

Data importer(s):

Name: **Expel, Inc.**

Address: 12950 Worldgate Dr, Suite 200 Herndon, VA 20170 USA

Contact person's name, position and contact details:

Peter Katz

VP, General Counsel and Data Protection Officer

email: privacy@expel.com

Activities relevant to the data transferred under these Clauses: Managed Detection and Response Services - provision of the Services by Data Importer on behalf of the Data Exporter as further described in the Vendor Agreement.

Role (controller/processor): **Processor**

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

- X **Customer customers and/or customers' end-users of an Customer product or service**
- X **Vendors or Vendors of Customer**
- X **Customer employees and/or staff**

☐ **Other:** (list here)

Data Access and Collection: [Select all that apply or **describe** if you select "other"]

- X **Customer will provide Vendor with the personal data**
- X **Vendor will collect the personal data directly from the data subject**
- ☐ Vendor is sourcing the personal data from another third-party

Categories of personal data transferred

[*Select all that apply or **describe** if you select "other"]*

- X **Contact Information** (e.g., name, email address, phone number, username, password)
- X **Location Data** (e.g., postal address, IP address, etc.)
- ☐ **Transactional Data** (e.g., purchase history, returns, payment information, etc.)
- ☐ **Preference Data** (e.g., profile/account settings, buying pattern, interest in specific topics, etc.)
- X **Employment Data** (e.g., title, employers, resume/CV, educational history, professional training, etc.)
- X **Other** (list here):
  - Email address
  - Company Name
  - IP address
  - URLs accessed by a device (for the purposes of investigation, not profiling)
  - Geolocation
  - Device/asset identifiers
  - Customer system username
  - Host name
  - Full name (associated with an IP address)
  - Data on anomalous system activity

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training),

keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A - No sensitive data and no Special Categories of Data are applicable

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Transfers would occur on a continuous basis

Nature of the processing

The nature and purposes of processing carried out by the Data Importer on behalf of the Data Exporter shall be as set out in the Vendor Agreement, and may include any or all of the following purposes:

Managed Detection and Response Services

Purpose(s) of the data transfer and further processing

The nature and purposes of processing carried out by Vendor on behalf of Customer shall be as set out in the Vendor Agreement, and may include any or all of the following purposes:

Managed Detection and Response Services

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Data Importer will process Customer Data until expiration or termination of the Vendor Agreement and for so long after such expiration or termination as required by law.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The nature and purposes of transfers to subprocessors are carried out by Vendor on behalf of Customer shall be as set out in the Vendor Agreement, and may include any or all of the following purposes:

Managed Detection and Response Services

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

- Irish Data Protection Commission (DPC)

This section is applicable only to data processing governed by European Union law

Exhibit 2

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

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (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 for the rights and freedoms of natural persons.

As further set forth in Section 5 of the DPA, and in addition to the security obligations set forth in the DPA, Vendor shall employ the following Technical and Organization Security Measures:

The **Data Exporter,** also known as the **'Customer**,' takes information security seriously and this approach is followed through in its processing and transfers of personal data. This information security overview applies to the **Data Importer** (also known as '**Expel, Inc.'** and the **'Vendor')** and their corporate controls for safeguarding personal data which is processed and transferred amongst the Vendor's group companies. Vendor's information security program enables the workforce to understand their responsibilities. Some solutions may have alternate safeguards outlined in the applicable order or other Contracts as agreed with Customer or the applicable Customer Subsidiary.

Security Practices

Vendor has implemented corporate information security practices and standards that are designed to safeguard Vendor's environments and to address business objectives across the following areas:

(1) information security
(2) system and asset management
(3) development, and
(4) governance.

These practices and standards have been approved by the Vendor's executive management and are periodically reviewed and updated where necessary.

Vendor shall maintain an appropriate data privacy and information security program, including policies and procedures for physical and logical access restrictions, data classification, access rights, credentialing programs, record retention, data privacy, information security and the treatment of personal data and sensitive personal data throughout its lifecycle. Key policies should be reviewed at least annually.

Organizational Security

It is the responsibility of the individuals across the Vendor's organization to comply with these practices and standards. To facilitate the corporate adherence to these practices and standards, Vendor's Information Security ("**IS**") function is responsible for the following activities:

1. **Security strategy** – the IS function drives Vendor's security direction. The IS function works to ensure compliance with security related policies, standards and regulations, and to raise awareness and provide education to users. The IS function also carries out risk assessments and risk management activities, and manages contract security requirements.

2. **Security engineering** – the IS function manages testing, design and implementation of security solutions to enable adoption of security controls across the environment.

3. **Security operations** – the IS function manages support of implemented security solutions, monitors and scans the environment and assets, and manages incident response.

4. **Forensic investigations** – the IS function works with Security Operations, Legal, Privacy, and Human Resources to carry out investigations, including eDiscovery and eForensics.

5. **Security consulting and testing** – the IS function works with software developers on developing security best practices, consults on application development and architecture for software projects, and carries out assurance testing.

Asset Classification and Control

Vendor's practice is to track and manage key information and physical, software and logical assets. Examples of the assets that Vendor might track include:

- information assets, such as identified databases, disaster recovery plans, business continuity plans, data classification, backups/backup operations, data retention requirements, and archived information
- software assets, such as identified applications and system software
- physical assets - desktops/laptops, printers, and communications equipment.

The assets are classified based on business criticality to determine confidentiality requirements. Industry guidance for handling personal data provides the framework for technical, organizational and physical safeguards. These safeguards may include controls such as access management, encryption, logging and monitoring, and data destruction.

Employee Screening, Training and Security

1. **Screening/background checks:** As part of the employment/recruitment process, Vendor shall perform or have performed screening/background checks on employees (which shall vary from country to country based on local laws and regulations), and on employees of subcontractors where such employees will have access to Vendor's networks, systems or facilities.

2. **Identification:** Vendor shall require all employees to provide proof of identification and any additional documentation that may be required based on the country of hire or if required by other Vendor entities or customers for whom the employee is providing services.

3. **Training:** Vendor's compliance training program includes a requirement for employees and contractors to complete information security and privacy awareness training when they onboard at Vendor followed by continuous security and privacy awareness videos that are watched by all employees and contractors on a monthly basis. The security and privacy awareness trainings provided by Vendor may also provide materials specific to certain job functions.

4. **Confidentiality:** Vendor shall ensure its employees are legally bound to protect and maintain the confidentiality of any personal data they handle pursuant to standard agreements.

Physical Access Controls and Environmental Security

1. **Physical Security Program:** Vendor shall use a number of technological and operational approaches in its physical security program to mitigate security risks to the extent reasonably possible. Vendor's security team works closely with each site to determine appropriate measures are in place to prevent unauthorized persons from gaining access to systems within which confidential information (including personal data) is processed and continually monitor any changes to the infrastructure, business and known threats. They also monitor best practice measures used by others in the industry and carefully select approaches that meet both uniqueness in business practice and expectations of Vendor. Vendor balances its approach towards security by considering elements of control that include architecture, operations and systems.

2. **Physical Access controls:** Physical access controls/security measures at Vendor's facilities/premises are designed to meet the following requirements:

   (a) access to Vendor's buildings, facilities and other physical premises shall be controlled and based upon business necessity, sensitivity of assets and the individual's role and relationship to the Vendor. Only personnel associated with Vendor are provided access to Vendor's facilities and physical resources in a manner consistent with their role and responsibilities in the organization;

   (b) relevant Vendor facilities are secured by an access control system. Access to such facilities is granted with an activated card only;

   (c) all persons requiring access to facilities and/or resources are issued with appropriate and unique physical access credentials (e.g. a badge or key card assigned to one individual) by the IS function. Individuals issued with unique physical access credentials are instructed not to allow or enable other individuals to access the Vendor's facilities or resources using their unique credentials (e.g. no "tailgating"). Unique credentials are non-transferable and if an individual cannot produce their credentials upon request, they may be denied entry to Vendor's facilities or escorted off the premises. At staffed entrances, individuals are required to present a valid photo identification or valid credentials to the security representative upon entering. Individuals who have lost or misplaced their credentials or other identification are required to enter through a staffed entrance and be issued a temporary badge by a security representative;

   (d) employees are regularly trained and reminded to always carry their credentials, store their laptops, portable devices and documents in a secure location (especially while traveling) and log out or shut down their computers when away from their desk;

   (e) visitors who require access to Vendor's facilities must enter through a staffed and/or main facility entrance. Visitors must register their date and time of arrival, time of leaving the building and the name of the person they are visiting. Visitors must produce a current, government issued form of identification to validate their identity. To prevent access to, or disclosure of, company proprietary information visitors are not allowed un-escorted access to restricted or controlled areas;

   (f) select Vendor facilities use CCTV monitoring, security guards and other physical measures where appropriate and legally permitted;

   (g) locked shred bins are provided on most sites to enable secure destruction of confidential information/personal data;

   (h) for Vendor's major data centres, security guards, UPS and generators, and change control standards are available;

   (i) for software development and infrastructure deployment projects, the IS function uses a risk evaluation process and a data classification program to manage risk arising from such activities.

Change Management

The IT organization manages changes to the corporate infrastructure, systems and applications through a centralized change management program, which may include testing, business impact analysis and management approval where appropriate. All relevant application and systems developments adhere to an approved change management process.

Security Incidents and Response Plan

1. **Security incident response plan:** Vendor maintains a security incident response policy and related plan and procedures which address the measures that Vendor will take in the event of loss of control, theft, unauthorized disclosure, unauthorized access, or unauthorized use or acquisition of personal data. These measures may include incident analysis, containment, response, remediation, reporting and the return to normal operations.

2. **Response controls:** Controls are in place to protect against, and support the detection of, malicious use of assets and malicious software and to report potential incidents to the Vendor's IS function or Service Desk for appropriate action. Controls may include, but are not limited to: information security policies and standards; restricted access; designated development and test environments; virus detection on servers, desktop and notebooks; virus email attachment scanning; system compliance scans; intrusion prevention monitoring and response; firewall rules; logging and alerting on key events; information handling procedures based on data type; e-commerce application and network security; and system and application vulnerability scanning. Additional controls may be implemented based on risk.

Data Transmission Control and Encryption

Vendor shall, to the extent it has control over any electronic transmission, transfer or storage of personal data, take all reasonable steps to ensure that such data cannot be read, copied, altered or removed without proper authority during its transmission, transfer or storage. In particular, Vendor shall:

1. implement industry-standard encryption practices in its transmission and storage of personal data. Industry-standard encryption methods used by Vendor includes Secure Sockets Layer (SSL), Transport Layer Security (TLS), a secure shell program such as SSH, and/or Internet Protocol Security (IPSec), and at least AES-256-bit encryption;

2. if technically feasible, encrypt all personal data, including, in particular any sensitive personal data or confidential information, when transmitting or transferring that data over any public network, or over any network not owned and maintained by Vendor. The Vendor's policy recognizes that encryption is ineffective unless the encryption key is inaccessible to unauthorized individuals and instructs personnel never to provide an encryption key via the same channel as the encrypted document;

3. for Internet-facing applications that may handle sensitive personal data and/or provide real-time integration with systems on a network that contains such information (including Vendor's core network), a Web Application Firewall (WAF) may be used to provide an additional layer of input checking and attack mitigation. The WAF will be configured to mitigate potential vulnerabilities such as injection attacks, buffer overflows, cookie manipulation and other common attack methods.

System Access Controls

Access to Vendor's systems is restricted to authorized users. Access is granted based on formal procedures designed to ensure appropriate approvals are granted so as to prevent access from unauthorised individuals. Such procedures include:

1. **admission controls** (i.e. measures to prevent unauthorized persons from using data processing systems):

    (a) access is provided based on segregation of duties and least privileges in order to reduce the risk of misuse, intention or otherwise;

    (b) access to IT systems will be granted only when a user is registered under a valid username and password;

(c) Vendor has a password policy in place which requires strong passwords for user login to issued laptops, prohibits the sharing of passwords, prohibits the use of passwords that are also used for non-work functions, and advises users on what to do in the event their password or other login credentials are lost, stolen or compromised;

(d) mandatory password changes on a regular basis or use of multifactor authentication (preferred);

(e) automatic computer lock, renewed access to the PC only after new registration with a valid username and password;

(f) data and user classification determine the type of authentication that must be used by each system;

(g) remote access and wireless computing capabilities are restricted and require that both user and system safeguards are in place as well as user authentication.

2. **access controls** (i.e. measures to prevent unauthorised access to systems):

(a) access authorization is issued in respect of the specific area of work the individual is assigned to (i.e. work role);

(b) adjustment of access authorizations in case of changes to the working area, or in case an employee's employment is terminated for any reason;

(c) granting, removing and reviewing administrator privileges with the appropriate additional controls and only as needed to support the system(s) in question;

(d) event logs from key devices and systems are centrally collected and reported on an exceptions basis to enable incident response and forensic investigations.

Data Access Control

Vendor applies the controls set out below regarding the access and use of personal data:

1. personnel are instructed to only use the minimum amount of personal data necessary in order to achieve the Vendor's relevant business purposes;

2. personnel are instructed not to read, copy, modify or remove personal data unless necessary in order to carry out their work duties;

3. third party use of personal data is governed through contractual terms and conditions between the third party and Vendor which impose limits on the third party's use of personal data and restricts such use to what is necessary for the third party to provide services.

Separation Control

Where legally required, Vendor will ensure that personal data collected for different purposes can be processed separately. Vendor shall also ensure there is separation between test and production systems.

Job Control

Vendor shall process personal data in accordance with the applicable services agreement between the Vendor and Customer and in accordance with the instructions of Customer. The following controls will be implemented by the Vendor:

1. personal data is processed only to the extent necessary for contractual performance;

2. personnel are subject to a written obligation of confidentiality;

3. diligent selection of (sub)processor and other service providers;

4. third party use of personal data is governed through contractual terms and conditions between the third party and Vendor which impose limits on the third party's use of personal data and restricts such use to what is necessary for the third party to provide services;

5. clear instructions to (sub)processors on security measures for protecting privacy including the appropriate technical and organizational measures to safeguard the personal data to the same or higher level of protection as provided by Vendor;

6. ongoing monitoring of (sub)processor's activities.

Availability Control

Vendor protects personal data against accidental destruction or loss by following these controls:

1. personal data is retained in accordance with customer contract or, in its absence, Vendor's record management policy and practices, as well as legal retention requirements;

2. hardcopy personal data is disposed of in a secure disposal bin or a crosscut shredder such that the information is no longer decipherable;

3. electronic personal data is given to Vendor's IT Asset Management team for proper disposal;

4. appropriate technical measures are in place, including (without limitation): anti-virus software is installed on all systems; network protection is provided via firewall; network segmentation; user of content filter/proxies; interruption-free power supply; regular generation of back-ups; fire safety system; water protection systems where appropriate; emergency plans; and air-conditioned server rooms provided by the Vendor's cloud hosting services providers.

Data Input Control

Vendor has, where appropriate, measures designed to check whether and by whom personal data have been input into data processing systems, or whether such data has been modified or removed. Access to relevant applications is recorded.

System Development and Maintenance

Publicly released third party vulnerabilities are reviewed for applicability in the Vendor environment. Based on risk to Vendor's business and customers, there are predetermined timeframes for remediation. In addition, vulnerability scanning, and assessments are performed on new and key applications and the infrastructure based on risk. Code reviews and scanners are used in the development environment prior to production to proactively detect coding vulnerabilities based on risk. These processes enable proactive identification of vulnerabilities as well as compliance.

Compliance

The information security, legal, and privacy compliance departments work to identify regional laws and regulations that may be applicable to Vendor. These requirements cover areas such as, intellectual property of the Vendor and its customers, software licenses, protection of employee and customer personal information, data protection and data handling procedures, trans-border data transmission, financial and operational procedures, regulatory export controls around technology, and forensic requirements.

Mechanisms such as the information security program, the executive privacy council, internal and external audits/assessments, internal and external legal counsel consultation, internal controls assessment, internal penetration testing and vulnerability assessments, contract management, security and privacy awareness training, security consulting, policy exception reviews and risk management combine to drive compliance with these requirements.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

When the Data Importer enters into a contractual relationship with a sub-processor, the technical and organizational measures agreed upon are no less than the technical and organizational measures agreed with the Data Exporter.