Data Transfer Impact Assessment

August 13, 2021

TIA Scope

Element's Data Transfer Impact Assessment ("TIA") addresses transfers within the scope of the GDPR. Specifically, the assessment covers the transfer of European data subjects' personal data when those data subjects use Element's US-based service.

TIA Methodology

The TIA:

- I) maps transfers of European data subjects' personal data to Element and its sub-processors in the U.S.;
- II) identifies the transfer tools Element relies on – the Standard Contractual Clauses;
- III) assesses the effectiveness of the Standard Contractual Clauses in light of the circumstances of the transfer, including a comparative analysis of the privacy protections afforded by U.S. and European law;
- IV) describes effective supplementary measures;
- V) identifies procedural steps to put those measures in place; and
- VI) describes how Element will continue to evaluate this TIA.

The analysis of privacy protections under U.S. laws focuses on laws applicable to the proposed transfer, what redress mechanisms are in place for the data importer and data subjects, and relevant practical experience regarding local authorities' requests to access the transferred data.

The analysis also takes into account the specific circumstances of the transfer, including the nature and type of data being transferred, affected data subjects, purposes of processing, and the sector in which the data importer operates.

Final Determination

As set out below, the risk associated with the proposed transfer is low: the transfer presents some risk due to shortcomings in privacy protections afforded by U.S. law, but that risk can be accommodated by the Standard Contractual Clauses.

I. Step 1: Know your transfer

Transfers to processors and sub-processors

Element may use sub-processors to help fulfill its obligations, including to host its service and send out email updates. These sub-processors may have access to data subjects' information for the limited purpose of providing the service they have been contracted to provide. Element uses the following sub-processors:

Sub-Processor	Function
Azure	**Cloud Compute Services**
AWS	**Cloud Compute Services**
SendGrid	**Email services**
Intercom	**Online support, documentation, and chat bot**
Heap	**User engagement analytics**
LaunchDarkly	**Feature flagging, A/B Testing**

All of Element's sub-processors are in the United States. As set forth in its data processing addendum, Element (i) requires its sub-processors to agree to provide protections to personal data that are at least as stringent as those Element agrees to provide in its data processing addendum and (ii) will notify its customers of any changes in Element's sub-processors and permit customers to object to such changes.

Categories of personal data being transferred

As set out in the data processing addendum, Element will process names, email addresses, and any other personal data customer transmits through Element's service. Element's service is not designed to process special categories of data.

Description of data subjects concerned by the data transfer

Data subjects include customers employees, contractors, and other authorized users of Element's service ("Users").

Purposes of the intended data processing

Element processes personal data to authenticate Users' access to the service.

Data minimization

Element processes the minimum amount of personal data necessary to authenticate Users' access to the service. In addition, Element processes data to improve the service only *in the aggregate and on an anonymized basis*.

Data storage

Element uses commercially reasonable and industry-standard physical, managerial, and technical safeguards to preserve the integrity and security of personal data. Element encrypts personal data in-transit and at rest using industry-standard encryption. Element also guards against common web attack vectors, hosts data in secure data centers, and implements firewalls and access restrictions on its servers to protect and secure its network.

II. Step 2: Applicable transfer tool

The Standard Contractual Clauses are the applicable transfer tool.

III. Step 3: The Standard Contractual Clauses Effectively Ensure A Sufficient Level Of Protection

1. Part One: Overview of U.S. Data Protection Requirements

Element is headquartered and processes personal data in the U.S. Federal, state, and local privacy law, businesses' public-facing representations about their privacy practices, and contractual commitments between businesses and third parties (collectively, "Data Protection Requirements") govern businesses' processing of personal data in the U.S. and obligate businesses to protect personal data against unauthorized processing. Data Protection Requirements in the U.S. are publicly available and sufficiently clear.

Federal Law

The Federal Trade Commission, using its enforcement powers under Section 5 of the FTC Act, protects consumer privacy and promotes data security by prohibiting unfair or deceptive practices in relation to personal data. FTC enforcement requires companies to implement reasonable privacy and information security practices, be transparent about their data processing activities, and adhere to any public representations they make about data protection.

Federal law also provides industry-specific rules that offer additional, robust protections for specific categories of sensitive data, such as personal data handled by healthcare providers (the

Health Insurance Portability and Accountability Act, "HIPAA"), credit rating agencies (the Fair Credit Reporting Act, "FCRA"), and financial institutions (the Gramm-Leach-Bliley Act, "GLBA").

Other federal laws such as the Telephone Consumer Protection Act ("TCPA") and Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM") govern direct marketing and other communications practices, and provide consumers with additional rights and choices with respect to businesses' use of personal data.

In addition, certain federal laws provide legal requirements for and limitations on the collection of information by the U.S. government for law enforcement and national security purposes, such as the Electronic Communications Privacy Act ("ECPA"), which includes the Wiretap Act, the Stored Communications Act ("SCA"), and the Pen Register Act, as well as the Foreign Intelligence Surveillance Act ("FISA"). The U.S. Constitution also limits interferences with individuals' rights to privacy. These rights often require a judge or magistrate to review and adjudicate executive branch requests for personal data.

With this legislation in place, the U.S. Privacy and Civil Liberties Oversight Board reviews the impact of U.S. governmental authorities' data collection efforts on privacy and civil liberties. The Federal Bureau of Investigation ("FBI") and the National Security Agency ("NSA") also maintain their own Privacy and Civil Liberties Officers who advise the agencies on privacy issues and ensure there are appropriate avenues to receive, investigate, and redress privacy or civil liberty complaints.

State Law

While state laws are primarily designed to protect their residents' personal data, in practice they establish national, if not international, data protection requirements for businesses because 1) many businesses do not have the resources to adequately segment their operations by jurisdiction and therefore must apply the most stringent legal requirements company-wide, and 2) state regulators can bring enforcement actions for business' conduct outside of the regulators' respective states, and out-of-state plaintiffs can bring actions against companies for not adhering to other states' data protection requirements.

Numerous state constitutions protect individuals' right to privacy and each state has enacted statutes protecting personal data. For example, every state has enacted consumer protection laws that are similar or provide more protections than the FTC Act described above. Every state has a law requiring private or governmental entities to notify individuals of security breaches involving certain types of personal data. Some states impose minimum information security requirements (*e.g.*, California, Virginia, and Massachusetts), and others have passed legislation offering enhanced protection for specific categories of particularly sensitive data. For example, Illinois' Biometric Information Privacy Act ("BIPA") and similar laws in Texas, Washington, California, New York, and Arkansas, regulate the processing of biometric data and Vermont has passed a law regulating the sale of personal data by businesses that lack direct relationships with the individuals to whom the data relate.

Further, states are beginning to pass general, omnibus privacy statutes governing various types of personal data processed within each state. For example, California passed the California Consumer Privacy Act ("CCPA") in 2018, which provides GDPR-like protections for information processed by businesses and incorporates fundamental data protection concepts found in European law. In 2020, California residents voted to pass the California Privacy Rights Act ("CPRA"), which provides even greater consumer privacy protections. Additionally, Virginia passed the Consumer Data Protection Act ("CDPA") in early 2021, which like the CCPA and CPRA, incorporates GDPR-like data processing principles.

Furthermore, individual data subjects whose information Element processes may bring common law tort claims. Most states recognize "privacy torts," which revolve around the principle recognized in the Restatement (Second) of Torts, that an individual should be able to lead, "to some reasonable extent, a secluded and private life." Privacy-related causes of action allow Element users to enforce adequate consumer privacy protections.

Contractual and Technical Restrictions

Element's data processing addendum requires Element to protect and safeguard customer data, including by imposing security and privacy controls as well as restricting processing activities. Customers can enforce terms of Element's data processing addendum through breach of contract litigation or by terminating their relationship with Element.

2. Part Two: Comparison Between U.S. Data Protection Requirements and E.U. standards

The color coded determinations in this section reflect the level of equivalency between privacy protections under European and U.S. law. These determinations do not reflect Element's compliance with the GDPR.

1. Basic data protection concepts

U.S. law meets E.U. standards.

As referenced above, the Data Protection Requirements incorporate basic data protection concepts and principles such as "personal data", "processing of personal data", "data controller", "data processor", "recipient", and "sensitive data".

For example, laws such as the CCPA, HIPAA, and GLBA include reference to and distinguish between data controllers and data processors, imposing varying obligations on each. Laws such as BIPA and CPRA provide additional safeguards for specific categories of sensitive information.

2. Lawful and fair processing for a legitimate purpose principle

U.S. law partially meets E.U. standards.

As referenced above, the Data Protection Requirements require that businesses process personal data in a lawful and fair manner.

For example, the FTC Act and similar state consumer protection laws prevent companies from engaging in unfair or deceptive acts or practices.

3. Purpose limitation principle

U.S. law meets E.U. standards.

As referenced above, the Data Protection Requirements require a company to process personal data for a specific purpose and to limit the company's subsequent use of this information for purposes compatible with initial purpose.

For example, laws such as HIPAA, GLBA, FCRA, and CCPA include purpose limitations for the processing of personal data.

4. Data quality and proportionality principle

U.S. law meets E.U. standards.

As referenced above, the Data Protection Requirements require that personal data must be accurate and kept up to date, as well as kept for an adequate, relevant, and limited time period in relation to the purposes for which it is processed.

For example, HIPAA, FCRA, and CCPA require that businesses maintain accurate information and offer data subjects the right to correct their data.

5. Data retention principle

U.S. law meets E.U. standards.

As referenced above, the Data Protection Requirements prevent businesses from retaining personal data for longer than is necessary for the purposes for which that information is processed.

For example, the recently passed CPRA and CDPA require service providers like Element to limit retention of personal data pursuant to the terms of their customer agreements.

6. Security and confidentiality principle

U.S. law meets E.U. standards.

As referenced above, the Data Protection Requirements require businesses to process personal data in a manner that ensures its security and maintains technical and organizational measures to safeguard personal data, including to protect it against unauthorized or unlawful processing and accidental loss, destruction, or damage.

For example, federal and state laws such as HIPAA, GLBA, FCRA, and CPRA require businesses to safeguard personal data. Similarly, state breach notification laws incentivize businesses to strengthen information security controls to mitigate the risk of cybersecurity incidents.

Moreover, Element maintains a record of known security incidents, including a description of the incident, the dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel. Appropriate resolution steps are identified and documented, including steps to minimize customer harm.

7. Transparency Principle

U.S. law meets E.U. standards.

As referenced above, the Data Protection Requirements incorporate the principle of transparency related to the processing of personal data by providing that individuals be informed of the main elements of the processing of their personal data in a clear, easily accessible, concise, transparent, and intelligible form.

For example, federal and state laws including HIPAA, GLBA, FCRA, CalOPPA, and CCPA require businesses to provide notices of their data processing activities to consumers.

As a processor, Element's notice obligations under the Data Protection Requirements are limited. However, it processes personal data as directed by its controller customers who are required to disclose their processing practices.

8. Data subject's rights

U.S. law partially meets E.U. standards.

As referenced above, the Data Protection Requirements offer data subjects some basic rights with respect to a business's processing of a data subject's personal data, including, to some extent:

- The right to obtain confirmation about whether data processing concerning him/her is taking place and to obtain a copy of that data
- The right to obtain rectification of his/her personal data as appropriate
- The right to obtain erasure of his/her personal data
- The right to object to processing on compelling legitimate grounds

For example, the CCPA and CPRA together provide individuals with a suite of data subject rights similar to those offered by the GDPR.

As a processor, Element is not directly responsible for responding to data subject rights requests but Element agrees in its data processing addendum to help its customers respond to such requests.

9. Restriction on onward transfer

U.S. law partially meets E.U. standards.

While U.S. federal and state law does not currently address onward transfers of data, Element's data processing addendum prevents Element from transferring European personal data to other countries without the approval of the initial data exporter.

10. Special categories of data

U.S. law meets E.U. standards; but this principle is not applicable to this transfer.

As referenced above, the Data Protection Requirements provide specific safeguards for sensitive data (defined in the GDPR as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation; personal data relating to criminal convictions and offenses).

For example, HIPAA provides enhanced protection for medical data and the Genetic Information Nondiscrimination Act protects genetic information in the context of health insurance and employment. State laws such as BIPA impose special consent and security requirements on businesses processing sensitive data (in the case of BIPA, biometric data). Additionally, state breach notification laws have specific notification requirements for data security incidents involving certain types of sensitive data, such as medical information.

Although this data would be protected under Data Protection Requirements, it is less of a concern in this assessment because Element is unlikely to process sensitive data. As stated in Element's data processing addendum, its services are not intended to process sensitive data.

11. Direct marketing

U.S. law meets E.U. standards.

As referenced above, the Data Protection Requirements allow data subjects to object to the processing of their data for direct marketing purposes.

For example, TCPA and CAN-SPAM Act permit individuals to object to certain kinds of prohibited marketing by telephone, text message, and email. GLBA provides individuals with the option to prohibit financial institutions from sharing their data with third parties for those parties' own marketing purposes. The CCPA and the CDPA grant individuals the right to opt out of the sharing of their data for a third party's own uses, including for direct marketing activities.

Additionally, companies that market their services often comply with the privacy recommendations of well-regarded self-regulatory regimes, such as the Digital Advertising Alliance. Internet browsers either block third-party advertising cookies or provide consumers with the option of blocking them altogether. The developers of these browsers are often creating new methods for users to protect their privacy.

Lastly, Element's data processing addendum prevents Element from using European residents' personal data for its own purposes, including for direct marketing to those individuals.

12. Automated decision making and profiling

U.S. law meets E.U. standards; however this principle is not applicable to this transfer.

The Data Protection Requirements allow data subjects to object to the processing of their data for automated decision making and profiling.

For example, the CPRA gives data subjects opt-out rights with respect to businesses' use of automated decision-making technology, which includes profiling individuals based on their performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements. In addition, at a consumer's request, businesses must disclose the logic involved in such decision-making processes.

Element does not process personal data based on automated decision-making or profiling.

3. Part Three: Procedural and Enforcement Mechanisms

1. Independent supervisory authority

U.S. law meets E.U. standards.

The U.S. has several independent supervisory authorities tasked with monitoring, ensuring and enforcing compliance with data protection and privacy provisions.

A few states have a data privacy supervisory authority (*e.g.*, California) or a division within the state's respective attorney general's office dedicated to data privacy and security (*e.g.*, Massachusetts). Otherwise, the FTC (and in some cases, other federal agencies) as well as state attorneys general enforce consumer protection, information security, and data breach notification laws.

2. Accountability

U.S. law meets E.U. standards.

As referenced above, the Data Protection Requirements ensure a high degree of accountability to and awareness of privacy and data protection obligations among controllers and those processing personal data. The FTC holds companies accountable for unfair and deceptive

privacy and security practices. Additionally, through various mechanisms, federal and state regulatory authorities communicate and enforce the Requirements, as do customers, individuals, capital markets, and the media.

3. Compliance

U.S. law partially meets E.U. standards.

As referenced above, the Data Protection Requirements oblige those processing personal data to be able to demonstrate compliance with the Requirements in particular to the competent supervisory authority.

For example, in the event of an enforcement action, the FTC or other federal or state agency bringing the action requires companies to demonstrate compliance. Some states such as California, New York, and Massachusetts require companies to demonstrate their maintenance of written information security programs and public-facing privacy policies.

Lastly, Element's data processing addendum requires Element to demonstrate its compliance with the addendum and allows customers to audit Element's data protection practices on request.

4. Support to Data Subjects in the Exercise of their Rights and Appropriate Redress Mechanism

U.S. law meets E.U. standards.

As referenced above, the Data Protection Requirements ensure that data subjects can pursue legal remedies to enforce their rights rapidly and effectively.

For example, federal laws such as HIPAA, FCRA, and GLBA permit individuals to seek legal redress for data protection violations. Additionally, some states such as California permit individuals to seek redress for data protection violations in the event of a breach. Further, data subjects can lodge complaints with the FTC, state attorneys general, and other government agencies to prompt these agencies to bring enforcement actions against companies not in compliance with Data Protection Requirements.

Further, Element's data processing addendum requires Element as a processor to assist its customers in responding to data subject requests those customers receive as controllers.

4. Part Four: Essential Guarantees for Law Enforcement and National Security Access to Limit Interferences to Fundamental Rights

The color coded determinations in this section reflect the level of equivalency between privacy protections under European and U.S. law. These determinations do not reflect Element's compliance with European law.

1. Actual disclosure requests made by authorities

Element has never received a request to disclose personal data from public authorities.

Element has never received requests to disclose personal data from U.S. authorities. Based on direction provided by several experienced former federal law enforcement officials with relevant national security expertise, Element does not expect to receive such a request because Element does not provide communications services. FISA Section 702 can only compel "electronic communication service providers" to comply with requests for personal data and communication data is most commonly sought in connection with criminal and national security investigations. The account credentials collected by Element would be of little utility to a national security investigation.

As noted in the U.S. Government's September 2020 White Paper, "companies whose EU operations involve ordinary commercial products or services, and whose EU-U.S. transfers of personal data involve ordinary commercial information like employee, customer, or sales records, would have no basis to believe U.S. intelligence agencies would seek to collect that data."

2. Processing must be based on clear, precise, and accessible rules (legal basis)

U.S. law partially meets E.U. standards.

As referenced above, the Data Protection Requirements ensure that interferences with privacy and data protection rights are set out in clear and precise, accessible (*i.e.*, public) statutes, which contain:

- A description of the nature of the offenses which may give rise to a demand for electronic data or an order requirement electronic surveillance
- A definition of the categories of people that might be subject to such surveillance or demands for electronic data
- Limitations on the duration of such measures
- The procedures to be followed for examining, using, and storing the data obtained by authorities
- The precautions to be taken when communicating the data collected to other third parties

The relevant U.S. statutes regarding electronic surveillance and the process for obtaining electronic data, and the policy guidance promulgated in connection with such statutes, require a consideration of individuals' rights to privacy and data protection, including those of non-U.S. residents.

Additional safeguards are provided by the professional standards and review requirements applicable to U.S. law enforcement and intelligence agencies, which are legally obligated to identify, and obtain advance approval for, the information they collect and search. Requests for approval to collect and search information are reviewed by agency lawyers and overseen variously by agency inspectors general, legislative committees, and in many instances, federal judges.

3. Necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated

U.S. law partially meets E.U. standards.

As referenced above, the Data Protection Requirements ensure that any interference with the right to privacy and a business's data protection obligations must be necessary and proportionate to the legitimate law enforcement and/or national security objectives pursued. As noted above, this is achieved, in part, by subjecting such privacy interferences to prior review and approval by a judge or other effective, independent, and impartial overseer.

For example, in most cases, the U.S. Constitution and other U.S. federal laws require such governmental interferences to be preceded by a showing of necessity by the relevant government authority that then must be evaluated by an independent judicial officer. State constitutions and statutes largely adopt or supplement such protections.

However, in certain instances, EU data protection authorities have questioned the sufficiency and the effectiveness of the protections described above.

4. Processing must be subject to independent oversight

U.S. law partially meets E.U. standards.

As referenced above, the Data Protection Requirements ensure that most governmental interferences with the right to privacy and data protection are subject to effective, independent, and impartial review and approval.

Specifically, the U.S. Constitution and many U.S. federal laws subject governmental interference with an individual's privacy interests to legal review by an independent judicial officer.

However, in certain instances, EU data protection authorities have questioned the sufficiency and the effectiveness of these protections.

5. Effective remedies must be available to data subjects

U.S. law partially meets E.U. standards.

As referenced above, the Data Protection Requirements provide effective remedies against improper interferences with the right to privacy and data protection.

The U.S. Constitution and federal laws subject governmental requests for data to judicial review. Additionally the private companies / individuals receiving the requests are often afforded opportunities to challenge governmental requests for personal data.

In certain instances, however, the individuals whose data are implicated are not informed in advance and therefore do not have opportunities to challenge a judicial order permitting access to their personal data.

5. Part Five: International Commitments

The color coded determinations in this section reflect the level of equivalency between privacy protections under European and U.S. law. These determinations do not reflect Element's compliance with the GDPR.

U.S. law does not meet E.U. standards.

The U.S. has entered into a data sharing agreement with the UK. However, at present, the U.S. has not made any international commitments arising from legally binding conventions or instruments nor does it participate in multilateral or regional systems in relation to the protection of personal data (*e.g.*, Convention 108; etc.).

6. Part Six: Conclusion

As described above, it is unlikely that public authorities in the U.S. will access personal data transferred to Element. First, Element's customer list is not publicly available so it is doubtful that public authorities would know that one of Element's customers used Element's services. Second, User's names and work email addresses are often readily available on the internet so there would be little need for public authorities to seek such data from Element.

If Element did somehow find itself subject to a request to access personal data from public authorities, Element would notify affected customers to the extent permitted by law and pursue all reasonable legal mechanisms of resisting and limiting the disclosure.

Accordingly, the concerns EU data protection authorities have raised with respect to U.S. public authorities accessing personal data will not impinge on the effectiveness of the Standard Contractual Clauses as a transfer tool here and the transfer can proceed without supplementary measures.

IV. Step 4: Adopt supplementary measures

While Element does not believe that additional measures are necessary to facilitate the proposed data transfer, the company has taken the following measures out of an abundance of caution.

1. Contractual measures

Element offers its data processing addendum to all of its customers.

2. Organizational measures

Element maintains internal data governance policies that require all Element employees with access to personal data to comply with Element's data protection obligations or be subject to discipline up to and including termination.

3. Technical measures

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Element Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for ISO 27001 compliance.

Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key.

ii) Preventing Unauthorized Product Use

We implement industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The

technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services. We also implement an IDS/IDP at the application layer to prevent unknown traffic patterns within our applications.

Static code analysis: Security reviews of all deployable artifacts is performed before deployment and is designed to prevent identifiable software flaws.

Penetration testing: We maintain relationships with industry recognized penetration testing service providers for annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Employee roles are reviewed at least once every six months.

Background checks: All Element Analytics employees undergo a third-party background check prior to being extended an employment offer, in accordance with and as permitted by the applicable laws. All Element Analytics employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

b) Transmission Control

In-transit: HTTPS encryption (also referred to as SSL or TLS) is required for any internet facing applications. Our HTTPS implementation uses industry standard algorithms and certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: We designed our infrastructure to log extensive information about the system behavior, and other application requests. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.9% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is replicated across multiple availability zones.

Online replicas and backups: All databases are backed up and maintained using at least industry standard methods.

Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.

V. Step 5: Procedural Measures

The supplementary measures described in Step 4 above do not contradict and cannot be construed to restrict the rights and obligations in the Standard Contractual Clauses, nor do they otherwise lower the level of data protection. Accordingly, additional procedural steps are not required.

VI. Ongoing Evaluation

Element will re-evaluate this TIA (a) annually and (b) whenever there is a material change in its business practices affecting Element's processing of personal data.