GDPR REPORT

EXECUTIVE SUMMARY

Base64.ai Inc. is committed to customer privacy and transparency. To this end, we have determined to meet GDPR (General Data Protection Regulation).

We assert that Base64.ai Inc. has met the obligations under the regulation for data privacy and protection. In this document we describe the technical, operational and management controls applicable to meeting GDPR guidance, as well as associated cyber security practices.

Our report asserts that we have met the requirements for the 7 principles of GDPR:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality
7. Accountability

T**hese serve to protect the end user rights under the GDPR rights to:**

- Information
- Access
- Rectification
- Restriction of Processing
- Data Portability
- Object
- Avoid Automated Decision-Making

DATA PROTECTION OFFICER

Appointment of Key Staff

The following individuals are selected for the following role:

- **Ozan Bilgen, CEO (fills duties of CISO):** Responsibilities include providing direction, guidance, leadership, and support for securing the entire information systems environment. This includes overseeing and assisting applicable personnel in their day-to-day operations to secure the environment, and researching and developing information security standards for the organization as a whole.
- **Ozan Bilgen, CEO (fills duties of Risk and Compliance Officer):** Responsibilities include chairing the Risk Committee and will provide insight and guidance on the risk posture of the organization directly to the CEO or the Board of Directors. At least twice a year, the Risk and Compliance Officer will provide a report and recommendations to the Executive Committee.
- **Ozan Bilgen, CEO:** Ensures that the organization processes the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.
- **Ozan Bilgen, CEO (IRT coordinator):** Responsibilities for this individual include daily operational oversight of all incident response initiatives.

Security and Privacy Governance

Base64.ai Inc. has a security steering committee with oversight over information security, risk assessment, risk management, and privacy. This committee exercises the overall function of enabling secure cyber practices within the firm. This includes a commitment to information assurance. Cyber security and privacy policies, as well as standards, procedures, guidelines and other supporting documents, are established, maintained, disseminated throughout the organization. All staff learn of these documents at hire, and at least annually thereafter. Internal committees work to monitor the cyber and privacy landscapes, ensuring governance documents are reviewed and updated in a timely fashion but no less than annually.

Base64.ai Inc. has established partnerships that enable prompt responses to incidents, such as with law enforcement and with others in the information security and privacy arenas.

Compliance

Through the security steering committee Base64.ai Inc. commits to being compliant with SOC 2 and GDPR. The firm engages Laika to perform security assessments annually. The firm is also committed to hiring independent, accredited professionals to complete independent assessments.

SECURITY & ENCRYPTION

Configuration Management

Base64.ai Inc. uses CIS hardened images, as well as a formalized Development-Security Operations program to monitor configuration management.

Secure Engineering and Architecture

Base64.ai Inc. has committed to using secure methods of engineering and architecture. This includes separation of test, development and production elements of the information system. Industry recognized best practices such as security by design and privacy by design are implemented. A simple standardized terminology allows for easy recognition by external regulators and consultants. In accordance with cloud computing best practices, processing and storage capabilities are redundant across geography to the extent permitted by regulation.

Security Operations

Base64.ai Inc. maintains a security operations team which is the first line of response to any security abnormality.

Continuous Monitoring

Logs and system records from various elements of the operating environment are consolidated into a single source for ingestion by a log aggregation platform.

Cryptographic Controls

Cryptographic controls are essential to the protection of Base64.ai Inc. data. In every case, data is encrypted both at rest and in transit. All workstations are encrypted using Windows BitLocker or Macintosh File Vault. Transmissions of data over a connection are done through modern SSL or TLS connections only.

Endpoint Security

Endpoint security is a basic building block for our security and privacy posture. Embedded devices are required to undergo specialized requirements gathering and undergo a DPIA if necessary. Base64.ai Inc. employs the use of endpoint protection (against malware, spyware and viruses) as well as firewalls, and change tracking technology where appropriate. When necessary, we notify subjects about the collection of data through a visible or auditory alert, minimize data collected to that with a business need, and then only use that data for authorized uses.

Maintenance, Network Security, Physical and Environmental Security

Systems are regularly maintained and reviewed according to the information security policy. Network security measures are developed, maintained and updated at least annually or after any significant change. Physical and Environmental controls are monitored and regulated in accordance with industry best practices.

Web Security

Base64.ai Inc. uses an enterprise standard for web site security, which includes a Demilitarized zone to restrict traffic to authorized devices.

RISK MANAGEMENT & AND INCIDENT RESPONSE

Risk Management

Base64.ai Inc. retains a risk register, which contains entries from the business impact assessment, supply chain risk assessment, data protection impact assessment and the company's overall risk assessment. Each entry is assigned an owner and is updated regularly among the risk/oversight committee.

Incident Response

Base64.ai Inc. has created an incident response plan to investigate, contain, mitigate, minimize and analyze any bad event that shall occur. This process involves people processes and technologies. Incidents shall first be reported internally, through a process that is documented, tested and reviewed at least annually. Should incidents be of the nature, through the company's counsel, the organization shall contact external partners and providers, to include law enforcement and regulatory matter experts.

PERSONAL DATA

Collection

Base64.ai Inc. ensures data is collected only for the purposes and method described in the privacy notice and that collection, use, and sharing of Personal Information is permissible under their jurisdiction.

Data Classification and Handling

We work to robustly de-identify personally identifiable information whenever practical. We limit the use of Personal Information transmission within and outside our network to only those instances where the data elements transmitted are necessary for our business operations as disclosed to customers. Business partners must adhere to our same standards for data safekeeping. As such, production data is never used within testing or development environments. To maintain accurate data flows, any change to the data flowing through our system is documented in the Data Flow Diagram. This diagram is updated at every major change. The diagram is also reviewed at least annually as part of our commitment to data safeguards.

Use/Retention/Disposal

Base64.ai Inc. ensures that Personal Information is only retained for the duration specified to fulfill the purpose necessary, then disposes, destroys, or anonymizes the data.

- **Data Integrity:** Base64.ai Inc. is committed to ensuring that data entered by subjects is the same as data stored within the system
- **Data Masking:** Base64.ai Inc. commits to showing personal information in user readable methods when necessary to fulfill a business need
- **Data Quality Management:** Base64.ai Inc. has committed to de-identify data, as well as maintain the quality and utility of data collected under this program.

PRIVACY BY DESIGN

Asset Management, Capacity, and Performance

Base64.ai Inc. tracks all assets, to include workstations and cloud based computing modules. These are typically provided in high level diagrams, low level diagrams, as well as data flow diagrams. To plan for capacity limits, as well as to maintain optimal system performance Base64.ai Inc. uses monitoring tools to manage capacity.

Business Continuity and Disaster Recovery

Base64.ai Inc. is committed to maintaining its business operations, in face of any event. Base64.ai Inc. has studied the various impacts to the business through a business impact analysis document. This document is updated at least annually. After completing this exercise, the firm gathered stakeholders to create the business continuity and disaster recovery plan. In the BCPDR, the firm discusses coordination of activities to provide continued services to her customers.

Change management

Base64.ai Inc. is committed to providing not only cutting edge, but safe and reliable products. Therefore, we have committed to safe coding practices, tied together with effective technical and management controls for change management.

These controls include:

- A ticketing system to track all changes to production
- Changes to production undergo a series of automated tests, and must pass through three distinct environments (development, test and production).
- Use of production data is prohibited in test and development environments.
- Technical controls are in place so that a change requester cannot be the same as a change approver. Thus, a coordinated malfeasance is necessary to inject malicious code into the code base.

Human Resources

Base64.ai Inc. realizes that security and privacy must begin by hiring trustworthy and honorable people to represent us. Therefore, we have developed a sophisticated set of procedures around the hiring, and termination of employees, contractors and other staff which may have access to our data at any time. To this end, we require criminal, education, and where appropriate, credit background checks.

PRIVACY IMPACT ASSESSMENT (PIA) / DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Cloud Security

Cloud products are at the core of our offerings. Cloud products undergo the Data Protection Impact Analysis at least annually or when added to a new project.

Data Protection Impact Assessment

Protection of data, data subjects, and proper handling of data are critical for our success. We begin by performing a data protection impact assessment (DPIA) at least annually.

RECORDS OF PROCESSING ACTIVITIES (RPA)

Automation

Base64.ai Inc. has implemented automated mechanisms to support the records management policies and procedures.

Attribute Management

Base64.ai Inc. manages the attributes of data collected by data subjects.

System of Record Notice

Base64.ai Inc. has maintained a record of processing of personal information.

RIGHTS OF SUBJECT

Identification/Authorization/Authentication/Access Control

Base64.ai Inc. utilizes Google Cloud Platform for an identity store, that is appropriate to the firm's size and scope of data contained therein to provide identification (unique identifiers for each employee) authorization (fine grained access to each data source, as well as authentication (ensuring an employee proves the identity to a satisfactory degree).

Notice

Notice is provided at the first interaction with the company and at a predictable interval thereafter that describe clear easy to understand methods in which data are collected, used, sold or otherwise within the organization.

- **Purpose specification**: Purpose for the data collection pertaining to use, maintenance and sharing is disclosed.

Notice of Correction/Amendment

Data subjects may correct or amend personal data in a manner consistent with applicable law through the methods described in the privacy notice.

Choice and Consent

Consent is given in plain English to "opt in" to data collection as opposed to a complicated web to "opt out"

- **Just in Time Notice & Consent:** Base64.ai Inc. takes steps to ensure that processing of personal information is done only under the original circumstance in which consent was granted.

Data Subject Access Requests (DSAR)

Base64.ai Inc. has created a process for receiving and responding to complaints, questions, or concerns pertaining to data subjects and personal information.

Right of Access

Data subjects may access their Personal Information, in a manner consistent with applicable law, through methods described in the privacy notice.

Appeal

Data subjects may appeal any adverse/incorrect decisions through a process at Base64.ai Inc.

Right of Erasure

Through a mechanism specified in the privacy notice, data subjects may have their data erase, in part or in full.

Data Portability

Data subjects have the right to export personal information in a common method usable to other machine readers.

TRAINING & AWARENESS

Security Awareness and Training

Base64.ai Inc. employee's, contractors and other contingent staff are required to undergo security awareness training, and where applicable, PCI, OWASP, HIPAA and/or secure engineering/coding practices at hire and at least annually thereafter.

THIRD PARTIES

Third Party Management

Base64.ai Inc. carefully evaluates third parties prior to releasing any information for processing or storage. Third parties are subject to at minimum non-disclosure agreements, and may be subject to more restrictive covenants as determined by the supply chain positioning or risk posed.