Cosign AI

Privacy and Data Protection Policy

Purpose and Scope

In its everyday business operations Cosign AI makes use of a variety of personal data, including data about:

- Current, past and prospective employees
- Customers
- Users of and visitors to its websites
- Subscribers
- Other stakeholders

In collecting and using this data, the organization is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.
The purpose of this policy is to set out the relevant legislation and to describe the steps Cosign AI is taking to ensure that it complies with it. This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to Cosign AI systems.

Privacy and data protection policy

Applicable privacy legislation

The list below shows the main items of privacy legislation that apply to the countries (or groups of countries) and states within which Cosign AI operates.

- USA – California - California Consumer Privacy Act (CCPA)

Cosign AI has a legal obligation to comply with the provisions of this legislation at all times. Whilst there will be variations in these provisions, this policy establishes the key principles that are commonly required to be observed in such legislation.
Significant fines may be applicable if a breach is deemed to have occurred under the relevant privacy legislation, which is designed to protect the personal data of citizens of the country (or state, region or countries) involved. It is Cosign AI's policy to ensure that our compliance with applicable legislation is clear and demonstrable at all times.

Definitions

The definitions used within privacy legislation vary and it is not appropriate to reproduce them all here. However, the common terms used within this policy are as follows:

- Personal data: Any information that (a) can be used to identify the personal data principal to whom such information relates, or (b) is or might be directly or indirectly linked to a personal data principal.
- Personal data principal: Natural person to whom the personal data relates. This term is also referred to as data subject.
- Processing of personal data: Operation or set of operations performed upon personal data.*Examples of processing operations of personal data include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of personal data.*
- Data Controller: Privacy stakeholder (or privacy stakeholders) that determines the purposes and means for processing personal data other than natural persons who use data for personal purposes.
- Data Processor: Privacy stakeholder that processes personal data on behalf of and in accordance with the instructions of a data controller.

Principles relating to processing of personal data

There are a number of fundamental principles upon which most privacy legislation is based. These are summarized as follows [Please note these are based on the EU GDPR and may need to be adjusted if your applicable legislation is significantly different]:

1. **Lawfulness, fairness and transparency** - personal data shall be processed lawfully, fairly and in a transparent manner in relation to the personal data principal
2. **Purpose limitation** – personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. **Data minimization** – the personal data collected and stored shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

4. **Accuracy** – personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
5. **Storage limitation** – personal data shall be kept in a form which permits identification of personal data principals for no longer than is necessary for the purposes for which the personal data is processed
6. **Integrity and confidentiality** – personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures

Processing of special categories of 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 shall be prohibited. Exception to this restriction is only applicable by lawful exceptions including but not limited to processing necessary to: reasons of public interest, purposes of preventive medicine, and defense or exercise of a legal claim.

Cosign AI will ensure that it complies with all these principles both within processing and as part of the introduction of new methods of system processing such as new IT systems.

Rights of the individual

The personal data principal also has rights with regard to their personal data. These will generally consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights are supported by appropriate procedures within Cosign AI that allow the required action to be taken within the timescales stated in the applicable privacy legislation.

These timescales are shown in the list below [Please note these are based on the EU GDPR]:

- The right to be informed - When data is collected (if supplied by personal data principal) or within one month (if not supplied by personal data principal)
- The right of access - One month
- The right to rectification - One month
- The right to erasure - Without undue delay
- The right to restrict processing - Without undue delay
- The right to data portability - One month
- The right to object - On receipt of objection
- Rights in relation to automated decision making and profiling - Not specified

If Cosign AI does not take action on the request of the personal data principals, Cosign AI shall inform the personal data principal at the latest within one month of receipt of the request of the reasons for not taking action.

In cases where requests from a personal data principal are unfounded or excessive, Cosign AI may either: charge a reasonable fee taking into account the administrative costs of providing the information/communication/taking the action requested; or refuse to act on the request.

Furthermore, Cosign AI may request additional information necessary to confirm the identity of the personal data principal making the request. The information provided to personal data principals shall be comprehensible and in a clearly legible manner with an overview of the intended processing.

Moreover, Cosign AI shall take reasonable steps to inform relevant data controllers, data processors, and recipients (as applicable) of request of rectification/erasure/restriction of processing from the data principal, unless this proves impossible or involves disproportionate effort.

Lawfulness of processing

Depending on the legislation involved, there may be a number of alternative ways in which the lawfulness of a specific case of processing of personal data may be established. It is Cosign AI policy to identify the appropriate basis for processing and to document it, in accordance with the applicable legislation. The main options are described in brief in the following sections.

Consent

Where appropriate, Cosign AI will obtain consent from a personal data principal to collect and process their data. In cases of children being below the age specified in applicable legislation, parental consent will be obtained. Transparent information about our usage of their personal data will be provided to personal data principals at the time that consent is obtained and their rights regarding their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.
If the personal data is not obtained directly from the personal data principal, then this information will be provided to the personal data principal within a reasonable period after the data is obtained and definitely within one month.

Performance of a contract

Where the personal data collected and processed is required to fulfill a contract with the personal data principal, consent is not required. This will often be the case where the contract cannot be completed without the personal data in question, for example, a delivery cannot be made without an address.

Legal obligation

If the personal data is required to be collected and processed in order to comply with applicable law, then consent is not required. This may be the case for some data related to employment and taxation for example, and for many areas addressed by the public sector. For example, processing of personal data relating to criminal convictions and offenses or related security measures.

Vital interests of the personal data principal

In a case where the personal data is required to protect the vital interests of the personal data principal or of another natural person, then this may be used as the lawful basis of the processing. Cosign AI will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data. As an example, this may be used in aspects of social care, particularly in the public sector.

Task carried out in the public interest

Where Cosign AI needs to perform a task that it believes is in the public interest or as part of an official duty then the personal data principal's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

Legitimate interests

If the processing of specific personal data is in the legitimate interests of Cosign AI and is judged not to affect the rights and freedoms of the personal data principal in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

Privacy by design

Cosign AI has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of privacy issues, including the completion of one or more privacy impact assessments.
The privacy impact assessment will include:

- Consideration of how as well as what types of personal data will be processed and for what purposes
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing personal data
- What controls are necessary to address the identified risks and demonstrate compliance with applicable legislation

Use of techniques such as data minimization/pseudonymization/encryption will be considered where applicable and appropriate, including at the end of processing, and the mechanisms used to achieve them will be documented.

Where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, Cosign AI shall consult the supervisory authority prior to processing.

Contracts involving the processing of personal data

Cosign AI will ensure that all relationships it enters that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the applicable legislation.

International transfers of personal data

Transfers of personal data between countries will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the applicable legislation. This depends partly on the relevant authority's judgment (for example in the case of the GDPR, the European Commission) as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

Where an adequacy decision (or similar statement) does not exist for a destination country, an appropriate safeguard such as standard contractual clauses will be used, or a relevant exception identified as permitted under the applicable legislation.

Intra-group international data transfers will be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for personal data principals.

Data protection officer

A defined role of Data Protection Officer (DPO) is generally required under privacy legislation if an organization is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.
Based on these criteria, Cosign AI [requires/does not require] a Data Protection Officer to be appointed.

Breach notification

It is Cosign AI's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the applicable legislation, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, where required the relevant supervisory authority will be informed within the specified timeframe (for example, for the GDPR within 72 hours). If acting as a data processor, Cosign AI shall notify the data controller of the data breach security incident. This will be managed in accordance with our *Security Incident Response Policy* which sets out the overall process of handling information security incidents.

Under privacy legislation, the relevant authority may have the right to impose a range of fines, often based on a percentage of annual worldwide turnover or a specific amount, for infringements of the regulations.

Addressing compliance to applicable privacy legislation

The following actions are undertaken to ensure that Cosign AI complies at all times with the accountability principle of privacy legislation within the countries in which it operates:

- The legal basis for processing personal data is clear and unambiguous
- A Data Protection Officer is appointed with specific responsibility for data protection in the organization (if required)
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to personal data principals wishing to exercise their rights regarding personal data and such inquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
- Organization name and relevant details
- Purposes of the personal data processing
- Categories of individuals and personal data processed
- Categories of personal data recipients
- Agreements and mechanisms for transfers of personal data to other countries including details of controls in place
- Personal data retention schedules
- Relevant technical and organizational controls in place

These actions are reviewed on a regular basis as part of the management process concerned with privacy and data protection.

Exceptions

Cosign AI business needs, local situations, laws and regulations may occasionally call for an exception to this policy or any other Cosign AI policy. If an exception is needed, Cosign AI management will determine an acceptable alternative approach.

Enforcement

Any violation of this policy or any other Cosign AI policy or procedure may result in disciplinary action, up to and including termination of employment. Cosign AI reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Cosign AI does not consider conduct in violation of this policy to be within an employee's or contractor's course and scope of work.

Any personnel who is requested to undertake an activity that he or she believes is in violation of this policy must provide a written or verbal complaint to his or her manager or any other manager of Cosign AI as soon as possible.

The disciplinary process should also be used as a deterrent to prevent employees and contractors from violating organizational security policies and procedures, and any other security breaches.

Responsibility, Review, and Audit

Cosign AI reviews and updates its security policies and plans to maintain organizational security objectives and meet regulatory requirements at least annually. The results are shared with appropriate parties internally and findings are tracked to resolution. Any changes are communicated across the organization.

This document is maintained by Riya Fukui.

This document was last updated on May 8, 2026.