RISKX

Your data. Assured.

Data Privacy Policy

Table of Contents

RISKX
Your data. Assured.

Objective

Risk X respects the privacy of all its customers and takes the protection of personal information very seriously. The Data Privacy Policy communicates the requirements for collecting, storing, using and protecting information that can be associated with a specific natural or juristic person and can be used to identify that person ("personal information") uniquely.

Scope

The scope of the Data Privacy Policy covers the global operations of the business.

Definitions

Responsible Party
Responsible parties are individuals/entities that determine how and whether Personal Information is processed.

Data Operators
Data operators are individuals/entities that process Personal Information on behalf of a Responsible party.

Data Subjects
Data Subjects are the individuals to whom the Personal Data relates.

Personal Data
Personal Data is any information about an identifiable individual. Examples of Personal Data include (but are not limited to):

- Name, date of birth, and social security or other identity card number;
- Contact information such as mailing address, email address, and phone numbers;
- Credit card and financial account numbers;
- Health or medical information;
- Information contained in employee files, including employment history, evaluations, and information collected during the application and hiring process; and
- Information related to employee benefits, such as the names of dependents, beneficiaries, and insurance policy information.

Properly anonymised and de-identified or aggregate data is not Personal Data.

Process
Process is used very broadly to indicate performing any action on Personal Data, such as collecting, recording, organising, storing, transferring, modifying, using, retaining, or deleting.

Special Personal Data
Special Personal Data is Personal Data that relates to an identifiable person's health, finances, sexual orientation, religious beliefs, or criminal record.

Policy

Privacy protection is integral to Risk X's processing of Personal Data as it protects customers and let customers feel comfortable with sharing their information with Risk X. As such, the following shall be addressed:

Data Collection and Consent

1. Risk X collect and process Personal Data in many ways, including but not limited to:

    a. Customers when completing a contact form on the Risk X website – Name, Surname, Email Address, Company Name, Contact Number.

    b. Employees and applicants as part of their employment or application. This information may include job applications, employee records of training, documentation of performance appraisals, salary, and other employment records.

    c. Non-member guests who visit for certain activities.

Such processes should be designed to minimise the unnecessary collection or use of Personal Data. For instance, use a reference number in place of an ID number when possible. Likewise, the use of anonymised and de-identified or aggregated data is generally preferable to the use of Personal Data.

2. Risk X shall implement a process for requesting consent before the collection and processing of personal data,

    a. Personal Data shall not be collected from children without clear parental or legal guardian written consent.

3. The following shall be disclosed before collecting any personal data:

    a. The identity of the person or entity that is collecting the Personal Data (i.e., the Responsible party);

    b. The purpose(s) for which the Personal Data is to be processed or used;

    c. The methods by which the Personal Data is to be collected;

    d. The scope of Personal Data that may be collected (e.g., types, over what period); and

    e. The identity of anyone to whom the Personal Data may be disclosed or transferred.

Withdrawal of Consent

4. Risk X shall implement a withdrawal of consent process, subject to contractual and legal restrictions and reasonable notice.

Purpose Specification and Use Limitation

5. Risk X shall use personal data in a way that is compatible with the purposes for which it was collected or for a reasonably related purpose.

    a. If data needs to be used for another purpose or handled in a way that the Data Subject has not provided consent, Risk X shall obtain consent from the Data Subject for the new or different use.

6. Only Risk X staff and third parties working on behalf of Risk X with a legitimate business purpose, as required by their job role, may access or use personal data.

Data Subject Access

7. Risk X shall post a privacy notice on their website so that Data Subjects can contact the appropriate department with enquiries or complaints regarding the use of their Personal Data.

Data Accuracy

8. Risk X shall provide its best efforts to process accurate personal data.

    a. Risk X shall apply to the extent reasonably feasible, correct or destroy personal data upon request that is inaccurate/misleading/out-of-date.

    b. If Risk X does not correct, the request should be noted in the Data Subject's file to the extent feasible and explained to the Data Subject.

Data Retention

9. Risk X shall not keep Personal Data for longer than necessary for the purpose for which it was collected in line with the *Data Retention Policy.*

10. Risk X shall securely destroy/erase Personal Data from Risk X systems when no longer required to accomplish the purpose for which it was collected in line with the *Secure Disposal Policy.*

Security

11. Risk X shall take reasonable administrative, technical and physical measures to safeguard against unauthorised processing or use of Personal Data, and the accidental loss of, or damage to Personal Data in line with the *Information Security Policy.*

12. Computer workstations shall be locked when a workspace is unoccupied.

    a. Risk X shall implement an automatic screen lock policy after 5 minutes of inactivity.

13. All Risk X employees shall ensure that any sensitive/confidential information in hardcopy or electronic form is securely locked away in their work area at the end of each day and when they are expected to be gone for an extended period.

Sharing of Personal Data with Third Parties

14. Risk X may share the Personal Data with its corporate affiliates and third parties that provide services to Risk X to the extent such third parties are contractually required to follow Risk X standards and procedures, and to protect Personal Data by all relevant laws, regulations and rules, subject to any appropriate security measures and directions from Risk X. Refer to *Third Party Supplier Policy.*

    a. These requirements shall also apply to any subcontractors engaged by third parties.

Confidentiality

15. Risk X employees and third-party contractors may not disclose information made available on Risk X systems and networks, include other personnel, except as explicitly authorised by appropriate management. The duty of nondisclosure and confidentiality extends to interactions with third parties, including other employees, customers, business partners, and vendors.

Incident Reporting and Response

16. In the event of suspected theft, loss or unauthorised processing of Personal Data, Risk X shall take immediate steps to investigate and contain a security breach in line with the *Quality Manual and Incident Response Policy.*

Children's Information

17. Suppose Risk X intends to collect or use personal information from children under the age of 13 (GDPR) and under the age of 18 (PoPI). In that case, Risk X must first obtain the verifiable consent of their parents or guardians, such as through consent forms that the parent or guardian signs in person. Consent need not be obtained where their parents or guardians provide information about children.

Privacy Enquiries and Disputes

18. Risk X shall designate an individual to handle complaints and disputes regarding the use of Personal Data.

    a. Risk X shall inform the individuals from whom it collects Personal Data of a phone number or email address that they may contact for complaints or disputes about how their Personal Data is handled.

    b. These complaints and disputes shall be addressed by Risk X management, who may decide when consultation with legal counsel is appropriate in anticipation of potential litigation with the Data Subject.

    c. Internal processing of requests for legal counsel would be subject to attorney-client privilege and attorney work-product doctrine protections.

Training

19. Employees with access to Personal Data shall receive annual training on this Privacy Policy.

Compliance with and Modification of Procedures

20. Risk X employees who violate this Privacy Policy may be subject to disciplinary actions, up to and including termination of employment.

References

- Incident Response Policy
- Quality Manual

RISKX
Your data. Assured.