THIRDEYE

Data Protection

&

Privacy Policy

Version 1.0
Sep 20, 2022

TABLE OF CONTENTS

INTRODUCTION 2

1. DATA PROTECTION PRINCIPLES **2**

2. GENERAL PROVISIONS **3**

3. LAWFUL, FAIR AND TRANSPARENT PROCESSING **3**

4. LAWFUL PURPOSES **3**

5. DATA MINIMIZATION **3**

6. ACCURACY **3**

7. ARCHIVING / REMOVAL **4**

8. SECURITY **4**

9. BREACH **4**

10. ROLES AND RESPONSIBILITIES **5**

INTRODUCTION

The Data Protection and Privacy Policy ensures that ThirdEye Data gathers, stores, and handles customer data fairly, transparently, and with respect to individual rights.

1. DATA PROTECTION PRINCIPLES

The Organization (ThirdEye Data) is committed to processing data in accordance with its responsibilities under the Data Processing Agreement (DPA).

DPA requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the DPA in order to safeguard the rights and freedoms of individuals; and
f. 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."

2. GENERAL PROVISIONS

a. This policy applies to all personal data processed by the Organization.
b. The Responsible Person shall take responsibility for the Organization's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. The Organization shall register with the Information Commissioner's Office as an organization that processes personal data.

3. LAWFUL, FAIR AND TRANSPARENT PROCESSING

a. To ensure its processing of data is lawful, fair and transparent, the Organization shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the Organization shall be dealt with in a timely manner.

4. LAWFUL PURPOSES

a. All data processed by the Organization must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The Organization shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organization's systems.

5. DATA MINIMIZATION

a. The Organization shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. ACCURACY

a. The Organization shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. ARCHIVING / REMOVAL

a. To ensure that personal data is kept for no longer than necessary, the Organization shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.
c. Any data with Personal Information (i.e., name, email address, phone number, IP address, user location, user passwords) will be encrypted and stored securely until expiration or termination of the relevant agreement, whichever is later.
d. Any client Data in ThirdEye Data Product (any data provided, uploaded, or submitted by/from you to the product in the course of using the product, and data processed, stored, and presented in the product as a derivative of the transmitted data for your use) is kept for a minimum of the duration of the relevant agreement plus the time specified in the agreement for data retention.
e. Any Transactional Data of client is kept for until expiration or termination of the relevant agreement.

8. SECURITY

a. The Organization shall ensure that personal data is encrypted and stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorized sharing of information.
c. When personal data is deleted, this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. BREACH

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data, the Organization shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

10. ROLES AND RESPONSIBILITIES

a. Data owners are employees who have primary responsibility for maintaining information that they own, such as an executive, department manager or team leader.
b. Information Security Administrator is an employee designated by the IT management who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources.
c. Users include everyone who has access to information resources, such as employees, trustees, contractors, consultants, temporary employees and volunteers.
d. The Incident Response Team shall be chaired by an executive and include employees from departments such as IT Infrastructure, IT Application Security, Legal, Financial Services and Human Resources.

END OF POLICY