The Keyholding Company

Data Protection Policy

Contents

1 Introduction

This Data Protection Policy (this "policy") sets out the obligations of The Keyholding Company Limited ("TKC", "we", "us", "our") regarding data protection and the rights of individuals whose personal data we collect, use and process in the course of our business activities.

This policy should be read together with the following related documents:

a) TKC Personal Data Retention and Destruction Policy
b) TKC Data Subject Rights Procedure
c) TKC Data Breach Procedure
d) TKC DPIA Procedure

Compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action, up to and including termination of employment for serious offences.

2 Policy Statement

The Keyholding Company is committed to meeting its data protection compliance obligations as set out in General Data Protection Regulation (EU Regulation 2016/679) ("GDPR"), the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA18") (the "law").

TKC places high importance on respecting the privacy and protecting the personal data of individuals with whom we work including our clients, partners and employees. We are committed to the fair, lawful and transparent handling of personal data and to facilitating the rights of individuals. Our policy is to comply not only to the letter of the law, but also to the spirit of the law.

3 Purpose

The purpose of this document is to specify and communicate to all team members TKC's policy on data protection. In particular:

- To ensure data protection good practice across the business; and
- To ensure compliance with the UK GDPR and other applicable legislation and regulations relating to personal data.

This document outlines internal policy in respect of data handling, and is subject to the laws, rules and regulations by which TKC is governed.

In the event this policy allows TKC team members to exercise discretion, such discretion must be exercised within the confines of TKC statutory obligations and must not contravene any of its legal, accounting or other regulatory requirements.

4 Scope

This policy applies to all personal data processed by TKC whether held in electronic form or in physical records, and regardless of the media on which that data is stored. It applies to personal data we create and collect directly from individuals and to personal data provided to us by member organisations.

The Keyholding Company Limited is registered as a data controller with the Information Commissioner's Office, registration number Z2338566.

This policy applies to all TKC employees, workers and contractors ("personnel", "you", "your"). Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action, up to and including termination for serious offences.

5 Definitions

The following definitions apply across all TKC data protection policies, procedures and supporting documents:

Term	Description:
Accountability	A duty to answer to the success or failure of strategies, decisions, practices and processes.
Anonymisation	The process of removing all personal identifiers from Personal Data, to ensure that the individual is no longer identifiable.
Data Controller	A person, entity or organisation that determines the purposes and means of processing Personal Data.
Data Protection Officer	The Data Protection Officer is responsible for overseeing data protection strategy and implementation to ensure compliance with Data Protection Law.
Data Processor	A person, entity or organisation that processes Personal Data on behalf of a Data Controller.
Data Subject	Any natural person (individual) whose personal data is being processed.
Data Protection Impact Assessment (DPIA)	A DPIA is designed to help an organisation assess the risks associated with data processing activities that could compromise the rights and freedoms of individuals. It can be used to identify and mitigate risk associated with a product, service, business process or other organisational change.
Legitimate Interest Assessment (LIA)	Determines if people's data is being used in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
Personal data	Defined within the UK GDPR as Information that relates to an identifiable individual either directly or indirectly using a combination of other Information. The United Kingdom's Information Commissioner's Office also states: "Information which has had identifiers removed or replaced in order to pseudonymise the data is still personal data for the purposes of GDPR".
processing	Any operation or set of operations that is performed on personal data, such as collection, recording, organising, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, combination, restriction or erasure.
pseudonymisation	A Data minimisation technique, where the Information processed or stored relating to an individual can no longer be attributed to a specific individual without use or access to additional information that has been stored separately.
Data Subject Access Request (DSAR)	Individuals have the right to access their personal data. This is commonly referred to as subject access. Individuals can make a subject access request verbally or in writing. Organisations have one month to respond to a request.

Information Commissioner's Office (ICO)	An independent public body established in the UK responsible for monitoring the application of the UK GDPR, Data Protection Act 2018 and the Privacy & Electronic Communications Regulations.
UK GDPR	Has the meaning given to it in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

6 Responsibilities

Key data protection responsibilities within TKC are as follows:

- The Keyholding Company Board is accountable for ensuring we meet our data protection obligations;
- The CFO is responsible for implementing and enforcing this policy;
- The TKC Leadership team are responsible for ensuring that personnel under their management are made aware of adhere and to this policy;
- All personnel working with personal data over which they have decision making authority are responsible for ensuring it is kept securely, is accessible only to those who need to use it and is not disclosed to any third party without the authorisation of a member of the Board; and
- All personnel are required to read, understand and adhere to this policy when processing personal data on our behalf.

You should speak with your line manager to ask a question, or raise a concern, relating to this policy or data protection.

7 Data protection principles

The following data protection principles shall govern the processing of personal data by TKC:

Principle 1 - Fair, Lawful & Transparent

- *Personal data must be processed lawfully, fairly, and in a transparent manner in relation to the data subject.*

This means we must only collect and process personal data where it is lawful for us to do so. We must provide data subjects with privacy information (a "privacy notice") notifying them of the purposes for which we process their personal data at the time of collection, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party. The privacy notice must explain what processing will occur and must also include the information required by law.

Our external privacy notice is available at https://www.keyholding.com/privacy-policy/.

Our employee and other related privacy notices are available by contacting TKC on 0370 770 6886 or privacy@keyholding.com.

Principle 2 - Purpose Limitation

- *Personal data must only be collected and processed for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.*

This means the way we use personal data must match the description given in the privacy notice and be limited to what is necessary for those specific purposes.

Principle 3 - Data Minimisation

- *Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.*

This means we must collect and process only as much personal data as we need for the purposes of the processing (as set out in our privacy notice). Additional personal data must not be collected or saved, even if provided to us.

Principle 4 - Accuracy

- *Personal data must be accurate and kept up to date.*

This means we must check the accuracy of personal data when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, we must amend or erase that data, as appropriate, without delay.

Principle 5 - Storage Limitation

- *Personal data which permits identification of data subjects (i.e. data which has not been anonymised) must be kept for no longer than is necessary for the purposes for which the personal data are processed.*

This means personal data must not be kept for any longer than is necessary, and only used for the purpose for which it was collected. When the data is no longer required, we must securely erase or dispose of it without delay. Our Personal Data Retention and Destruction Policy defines how long data must be retained.

Principle 6 - Security

- *Personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.*

This means we must protect the personal data we collect and ensure that it is not disclosed to third parties without authorisation, is not altered without approval and remains available to individuals with permission to have access to it.

Principle 7 – Accountability

- *TKC shall be accountable for ensuring compliance with its data protection obligations under the UK GDPR and DPA18.*

TKC is responsible for meeting and demonstrating compliance with its data protection obligations as set out in the UK GDPR.

a) Records of Processing

Where required to do so by the UK GDPR, we will keep written internal "Records of Processing Activities" in respect of all personal data collection, holding, and processing. Our Records of Processing Activities ("RoPA") shall incorporate the information required by the UK GDPR at Article 30. The RoPA will incorporate the following information:

- The name and contact details of the data controller, the data protection officer ("DPO") (if applicable) and any joint controllers,
- The purposes for which we process personal data,
- Details of the categories of personal data collected, held, and processed by us; and the categories of data subject to which that personal data relates,
- Details (and categories) of any third parties that will receive personal data from us,

- Details of any transfers of personal data to countries outside the European Economic Area ("EEA") including all mechanisms and security safeguards,
- The envisaged retention periods for the different categories of personal data; and
- Descriptions of the technical and organisational measures we have implemented to ensure the security of personal data.

b) Data Protection Officer

TKC have appointed an external, independent Data Protection Officer ("DPO") for monitoring implementation and compliance with UK GDPR. The DPO is Evalian Limited. All enquiries relating to data protection should be emailed to privacy@Keyholding.com.

c) Data Protection by Design

We will implement data protection by design and by default when processing personal data. This will include implementing suitable organisational and technical safeguards to reduce the risks to data subjects associated with our processing activities. Safeguards will be implemented during the design, implementation, and lifetime of processing activities. Organisational safeguards shall include awareness training for all personnel and suitable policies and procedures relating to the processing of personal data. This risk led approach to data protection will be applied across all business activities to ensure data protection by design and by default.

d) Data Protection Impact Assessments

Where the risks to rights and freedoms of data subjects associated with any existing or planned personal data processing to be carried out are potentially high or where otherwise required by applicable law, we will carry out a Data Protection Impact Assessment ("DPIA"). All DPIAs are to be undertaken as set out in the TKC Data Protection by Design & DPIA Policy. A register of DPIAs shall be kept, to include details of the outcome, the names of the parties signing off the DPIA recommendations and the date of the next review.

e) Data Processor Contracts

Where we utilise a data processor, we will put a binding contract in place between TKC and the data processor to include, as a minimum, the contract terms required by the UK GDPR at Article 28.

f) Access to Data

Only those personnel that need access to, and use of, personal data in order to carry out their assigned duties correctly will be permitted access to the personal data we hold. All personnel handling personal data on our behalf must be:

- Made fully aware of their individual responsibilities under this policy and applicable law, and be provided with a copy of this policy,
- Appropriately trained to do so and suitably supervised, with training to be provided upon induction, with refresher training to be provided at least annually, and
- All consultants, agencies and other parties working on our behalf and handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as applicable to our personnel.

8 Data Protection by Design and Default

TKC shall ensure that the risks to rights and freedoms of data subjects associated with processing are key considerations when:

- Designing, implementing and during the life of business practices and processes that involve the processing of personal data ("processing activities"); and
- Developing, designing, selecting, procuring, and using applications, services, products and other IT systems and technologies for collecting, holding, sharing, accessing, and otherwise processing personal data ("processing systems").

This risk led approach to processing activities and processing systems shall apply throughout the full lifecycle of the processing, from initial planning and setting of specifications, during use of processing systems, through to disposal of the personal data. It shall take into account both the likelihood and the severity of the potential harm to individuals.

Where the risk to rights and freedoms of data subjects is likely to be high, or where otherwise required by law or the Information Commissioner's Office, a DPIA shall be performed.

Safeguards and preventive measures shall be implemented into processing activities and processing systems from the outset and throughout the processing lifecycle, to mitigate the risks to data subjects and protect their rights. These safeguards and measures shall be proportionate to the risks and include organisational (e.g. policy, awareness, governance, and assurance) as well as technical measures (e.g. pseudonymisation). The objectives of such safeguards and measures shall include;

- Data minimisation
- Limiting the extent of the processing, storage, and access to what is strictly necessary
- Ensuring transparency for data subjects regarding the processing activities; and
- Ensuring the security of the personal data

9 Data Protection Impact Assessments

TKC shall carry out a DPIA before, or when we plan to carry out any of the following activities as a data controller:

- Undertake any type of processing which is likely to result in a high risk to the rights and freedoms of data subjects
- Use systematic and extensive profiling based on automated processing with legal or similar significant effects on data subjects
- Process special category or criminal offence data on a large scale
- Systematically monitor publicly accessible places on a large scale; or
- Undertake any other processing activity in a country in which the Information Commissioner's Office has mandated that the processing activity necessitates a DPIA

DPIAs shall be undertaken as set out in the TKC DPIA Procedure and DPIA Template. These documents consist of a set of initial screening questions and depending upon the potential risks to the data subjects, may require the completion of a full DPIA.

A record of DPIAs shall be kept, to include details of the outcome, the names of the parties signing off the DPIA recommendations, and the date of next review.

10 International data transfers

TKC will only transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA where:

- The transfer is to a country (or an international organisation), that the European Commission has determined ensures an adequate level of protection,
- Standard Contractual Clauses adopted by the European Commission have been put in place between TKC and the entity located outside the EEA,
- Binding corporate rules have been implemented, where applicable, or
- The transfer is otherwise permitted by the UK GDPR.

11 Data subject rights

In addition to the right to be informed, which is facilitated by providing Privacy Notices as set out above, the UK GDPR grants specific rights to data subjects in respect of the personal data collected and processed by TKC as a data controller.

a) Right of Access

More commonly known as Data Subject Access Requests ("DSARs" or "SARs"), data subjects have the right to request and obtain information relating to, and to receive a copy of, their personal data.

b) Right to Rectification

Data subjects have the right to obtain the rectification or completion of inaccurate or incomplete personal data concerning him or her.

c) Rights to Erasure, Restriction, Data Portability and to Object

In certain circumstances and, in some cases, subject to specific exceptions, data subjects have the right to:

- Obtain the erasure of personal data concerning them,
- Obtain the restriction of processing of personal data concerning them,
- Obtain the personal data which they have provided to us, and have the right to transmit this data to another controller without hindrance, where technically feasible (data portability),
- Object at any time to processing carried out in our legitimate interests, or for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller or carried out for direct marketing purposes.

d) Automated Decision Making

Data Subjects have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or similarly significant affects concerning them.

e) Facilitating Data Subject Rights

TKC is required to provide within one month of receipt, information on the action we have taken to facilitate the request, or where applicable, the reasons for not taking action. This must include the data subject's right to lodge a complaint with the ICO and to seek a judicial remedy. The UK GDPR permits us to extend this period by a further two months in certain circumstances. Requests by data subjects to exercise their rights must be facilitated as set out in the TKC Data Subject Rights Procedure.

Because of the importance of facilitating data subject rights and to ensure we meet the deadlines for responding to requests, you must communicate receipt of a request from a data subject to exercise their rights without delay, by sending an email with details of the request to privacy@Keyholding.com.

A template for a Subject Access Request can be found in Schedule 1 of the TKC Data Subject Rights Procedure.

12 Data retention and disposal

Personal Data shall not be retained for longer than is reasonably required, and in any event only for as long as is set out in the TKC Data Retention and Destruction Policy.

Once personal data records have reached the end of their life, they must be securely destroyed in a manner that ensures that they can no longer be used. Hard drives of redundant computers should be removed and destroyed before disposal if they have been used to hold personal data.

13 Security, integrity and confidentiality

TKC shall implement appropriate technical and organisational measures to ensure the confidentiality, integrity, availability, and resilience of personal data. Such measures shall be proportionate to the risks to data subjects associated with the processing activities in question, and shall include (without limitation):

- Encryption and pseudonymisation of personal data where appropriate,
- Policies relating to information security, including the secure processing of personal data,
- Information security awareness training, including the secure handling of personal data,
- Business continuity and disaster recovery capabilities to ensure the ongoing availability of and access to personal data, and
- Processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organisational measures implemented to ensure the security of the processing.

14 Data breach notification

Personal data breaches must be reported immediately to privacy@Keyholding.com.

The Information Commissioner's Office must be notified of any breach within 72 hours after having become aware of it if the breach is likely to result in a risk to the rights and freedoms of data subjects. Data subjects must be notified of the breach without undue delay if the breach is likely to result in a high risk to their rights and freedoms.

All data breaches, including those which do not require notification to be provided to the Information Commissioner's Office, must be handled strictly in accordance with the TKC Data Breach Procedure and added to the TKC Data Breach Register, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

15 Protection of personal data

All personnel must comply with the following when working with personal data:

- Personal data must always be handled with care and must not be shared with any colleague or any third party without authorisation,
- Physical records must not be left unattended or in the view of unauthorised employees, agents, contractors, or other parties at any time and must not be removed from the business premises without authorisation,
- If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period, the user must lock the computer and screen before leaving it,
- All physical copies of personal data, along with any electronic copies stored on physical, removable media, should be stored securely in a locked filing cabinet, drawer, box or similar,
- All electronic copies of personal data are to be stored securely using passwords which are changed regularly, and which do not use words or phrases that can be easily guessed or otherwise compromised,
- Personal data must not be transferred to any device personally belonging to an employee or transferred or uploaded to any personal file sharing, storage, communication, or equivalent service (such as a personal cloud service),
- Personal data may only be transferred to devices belonging to agents, contractors, or other parties working on our behalf where the party in question has agreed to comply fully with the letter and spirit of this policy and the law (which may include demonstrating that all suitable technical and organisational measures have been taken or entering into a data processor contract),
- All personal data stored electronically shall be backed-up regularly and securely, and
- Under no circumstances must any passwords be written down or shared between any employees, agents, contractors, or other parties working on our behalf, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

16 Implementation and Policy Management

This procedure shall be reviewed annually and following any personal data breach by the CFO and DPO.

Signed

Charlie Gordon Lennox – CEO Date: 31 January 2024