

KPEA (UK) LIMITED - DATA PROTECTION AUDIT AND INFORMATION GOVERNANCE REVIEW

Last Reviewed: July 2026

1. INTRODUCTION

This Data Protection Audit has been undertaken to ensure that KPEA (UK) Limited maintains appropriate systems, procedures and safeguards for the collection, processing, storage, sharing, retention and destruction of personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable legislation.

KPEA (UK) Limited provides process serving, tracing, investigation and related legal support services throughout the United Kingdom. In carrying out these services, personal data is processed on behalf of solicitors, businesses, public bodies and private individuals.

The purpose of this audit is to document how personal data is obtained, processed, secured and managed throughout the business and to demonstrate compliance with applicable data protection legislation.

2. BUSINESS OVERVIEW

KPEA (UK) Limited operates as a specialist enquiry agency and legal support services provider.

The company maintains a network of approved agents throughout the United Kingdom who undertake assignments on an agency basis. These agents do not have access to KPEA's internal systems and are only provided with the specific personal data necessary to complete individual instructions.

Access to KPEA's systems and electronic records is restricted to two authorised employees.

Lorna Bevins is responsible for data protection compliance within the business.

3. SOURCES OF PERSONAL DATA

Personal data is received from a variety of sources including:

- Solicitors, law firms and legal professionals instructing KPEA on behalf of their clients;
- Commercial organisations requiring tracing, investigation or process serving services;
- Private individuals instructing KPEA directly;
- Approved agents acting on behalf of KPEA;
- Publicly available information sources where lawful and appropriate;
- Information obtained during the course of investigations, tracing activities and process serving assignments.

4. CATEGORIES OF PERSONAL DATA PROCESSED

The personal data processed by KPEA will vary depending upon the nature of the instruction received and may include:

- Personal identification details;
- Contact details;
- Family and relationship information;
- Employment and educational information;
- Financial information;
- Property information;
- Investigation notes and reports;
- Process serving records;
- Tracing information;
- Photographs and video recordings;
- Witness statements and evidence;
- Litigation-related information.

Where necessary and lawful, KPEA may also process special category data or information relating to criminal allegations, proceedings or convictions where required for the establishment, exercise or defence of legal claims or where another lawful basis applies.

5. LAWFUL BASIS FOR PROCESSING

KPEA processes personal data under one or more of the following lawful bases:

- Performance of a contract;
- Compliance with legal obligations;
- Legitimate interests pursued by KPEA or its clients;
- Establishment, exercise or defence of legal claims;
- Other lawful bases as permitted under UK GDPR and the Data Protection Act 2018.

KPEA acts either as a data processor or an independent data controller depending upon the nature of the instruction and the contractual relationship with the client.

6. COLLECTION, STORAGE AND SECURITY OF PERSONAL DATA

6.1 ELECTRONIC SYSTEMS

Instructions are received by email, post, telephone and secure electronic means.

Electronic records, documents, photographs, videos and case-related information are stored using Microsoft 365 Business Premium and Microsoft OneDrive for Business.

Access to all systems is controlled through a single user account.

Multi-factor authentication is enabled on all Microsoft 365 accounts.

All company computers and laptops are protected using Microsoft BitLocker encryption and are secured by password-protected user accounts.

Microsoft provides encryption of data both in transit and at rest within its cloud infrastructure.

6.2 EMAIL SECURITY

KPEA uses Microsoft Exchange Online as part of Microsoft 365 Business Premium.

Email security controls include:

- Multi-factor authentication;
- Anti-malware protection;
- Anti-spam filtering;
- Microsoft Defender security services;
- Secure encrypted transmission of data.

Authorised personnel may access company email accounts on mobile devices which are protected through passcodes, biometric authentication and remote wipe functionality.

6.3 CYBER SECURITY

KPEA maintains appropriate technical measures to protect personal data, including:

- Endpoint security software;
- Device encryption;
- Secure password policies;
- Multi-factor authentication;
- Firewall protection;
- Regular software and security updates;
- Access control procedures;

- Secure cloud storage and backup facilities.

6.4 PHYSICAL SECURITY

Paper files continue to be maintained where necessary.

Physical records are stored in locked fire-resistant metal filing cabinets located within a dedicated office.

The office forms part of the home address of the company's director but is physically separate from the residential accommodation and protected by lockable access points.

Access to physical records is restricted to authorised personnel only.

Confidential waste documents are securely shredded before disposal.

7. SHARING PERSONAL DATA

KPEA shares personal data only where necessary to fulfil client instructions or comply with legal obligations.

Personal data may be shared with:

- Approved process servers;
- Approved tracing agents;
- Approved investigators;
- Solicitors and legal professionals;
- Courts, tribunals and regulatory bodies;
- IT service providers where necessary for system maintenance and support.

Agents are provided only with the information necessary to complete the specific task assigned to them.

KPEA takes reasonable steps to ensure that third parties receiving personal data understand their obligations regarding confidentiality and data security.

8. DATA PROTECTION IMPACT ASSESSMENTS

KPEA reviews the nature of each service and instruction to determine whether a Data Protection Impact Assessment (DPIA) is required.

Most tracing and process serving activities do not require a formal DPIA.

Where surveillance, covert investigations or other higher-risk processing activities are undertaken, KPEA assesses whether a DPIA is required before processing begins and implements appropriate safeguards where necessary.

9. DATA SUBJECT RIGHTS

KPEA recognises and supports the rights of individuals under UK GDPR including:

- Right to be informed;
- Right of access;
- Right to rectification;
- Right to erasure where applicable;
- Right to restrict processing;
- Right to data portability where applicable;
- Right to object;
- Rights relating to automated decision making.

Requests relating to personal data are handled in accordance with KPEA's Privacy Notice and Subject Access Request procedures.

10. DATA BREACHES

All staff and agents are required to report actual or suspected data breaches immediately upon becoming aware of them.

KPEA maintains procedures for:

- Investigating data breaches;
- Assessing risk to affected individuals;
- Recording breaches;
- Reporting notifiable breaches to the Information Commissioner's Office within statutory time limits;
- Notifying affected individuals where required.

11. INTERNATIONAL TRANSFERS

KPEA primarily stores personal data within the United Kingdom and approved Microsoft cloud environments.

Where personal data is transferred outside the United Kingdom, KPEA will ensure that appropriate safeguards are in place in accordance with UK GDPR requirements.

12. RETENTION OF RECORDS

KPEA retains personal data only for as long as necessary to fulfil the purposes for which it was collected and to satisfy legal, regulatory and contractual obligations.

Case files are normally retained for a period of ten years following closure of the matter.

This retention period enables KPEA to respond to legal claims, contractual disputes, regulatory enquiries and professional obligations.

At the end of the retention period, records are securely destroyed or permanently deleted unless a lawful reason exists for further retention.

13. TRAINING AND AWARENESS

KPEA ensures that authorised personnel remain aware of their data protection responsibilities and understand the importance of protecting personal data.

Data protection obligations form part of KPEA's operational procedures and are regularly reviewed.

14. REVIEW

This audit will be reviewed periodically and updated whenever significant changes occur to KPEA's business activities, systems, technology or legal obligations.

KPEA (UK) Limited

July 2026