KAIZEN
CERTIFICATION

Data Protection Policy

November 2025

Contents

1. Introduction to Data Protection....2
2. Scope and Applicability....4
3. Compliance with Legislation....6
4. Principles of Data Handling....8
5. Data Security Measures....10
6. Data Sharing and Disclosure....12
7. Data Subject Rights....14
8. Data Breach Response....16
9. Training and Awareness....18
10. Record Retention and Disposal....20
11. Policy Review and Updates....22
12. Compliance Monitoring and Auditing....24

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

1. Introduction to Data Protection

Purpose and Scope

Kaizen Certification Ltd is dedicated to respecting and protecting the privacy and data of our clients, employees, and stakeholders. This Data Protection Policy outlines our commitment to data protection and privacy in accordance with the General Data Protection Regulation (GDPR) and the UK Data Protection Act. The policy covers all data, whether digital or paper-based, that we collect, store, process, and share, ensuring it is handled lawfully, transparently, and securely.

Commitment to Data Protection

At Kaizen Certification Ltd, we recognise the importance of protecting personal data and the privacy of individuals. We are committed to:

- Processing personal data lawfully, fairly, and in a transparent manner.
- Collecting data for specified, explicit, and legitimate purposes and not processing it further in a manner incompatible with those purposes.
- Ensuring that data is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.
- Maintaining the accuracy of data and, where necessary, keeping it up to date.
- Keeping data in a form which permits identification of data subjects for no longer than is necessary.
- Processing data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

GDPR Compliance

Our policy and practices are in line with the requirements of the GDPR, which provides a framework for data protection laws across Europe, and the UK Data Protection Act. These regulations grant individuals greater control over their personal data and offer clear guidelines for its management. We are dedicated to upholding these standards in every aspect of our business.

Responsibility and Governance

Data protection is a responsibility shared across our entire organisation. Every employee of Kaizen Certification Ltd who interacts with data is obliged to adhere to this policy and the procedures that support it. We have appointed a Data Protection Officer (DPO) responsible for overseeing our data protection strategy and implementation to ensure compliance with GDPR requirements.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

Policy Application

This policy applies to all personal data processed by Kaizen Certification Ltd, regardless of where the data is stored or who owns it. It includes data processed on clients, employees, partners, and other individuals the company interacts with.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

2. Scope and Applicability

Scope of the Policy

This Data Protection Policy applies to all personal data processed by Kaizen Certification Ltd. 'Personal data' refers to any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, or an online identifier. This policy encompasses all data, whether held electronically, on paper, or other materials.

Applicability to Data Subjects

The policy applies to the data of a wide range of individuals, including but not limited to:

- Clients and customers of Kaizen Certification Ltd.
- Employees and job applicants.
- Contractors, service providers, and business partners.
- Other individuals who may come into contact with Kaizen Certification Ltd.

Applicability Across Operations

The Data Protection Policy applies to all operations and business processes of Kaizen Certification Ltd that involve the collection, processing, storage, and sharing of personal data. This includes, but is not limited to:

- Client management systems.
- Employee records and HR systems.
- Marketing activities and client communications.
- Digital platforms including websites and mobile applications.
- Financial and transactional systems.

International Data Transfers

In instances where personal data is transferred outside of the European Economic Area (EEA), Kaizen Certification Ltd will ensure such transfers comply with the applicable data protection laws. This includes ensuring that similar levels of data protection are maintained and that appropriate safeguards are in place.

Roles and Responsibilities

All employees, contractors, and other individuals working on behalf of Kaizen Certification Ltd are responsible for adhering to this policy and for ensuring that the personal data they handle is processed in accordance with the applicable data protection laws and principles.

Data Processing Activities

This policy governs all activities involving the processing of personal data, including but not limited to:

- Collection and recording of data.
- Storage and organisation of data.
- Adaptation or alteration of data.
- Retrieval and consultation of data.
- Use or application of data in business processes.
- Disclosure or transmission of data.
- Erasure or destruction of data.

Third-Party Data Processors

Where third parties process data on behalf of Kaizen Certification Ltd, they are required to comply with this policy and the relevant data protection legislation. Contracts with third-party processors will explicitly outline their data protection responsibilities.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

3. Compliance with Legislation

Legal Framework

Kaizen Certification Ltd is committed to full compliance with all applicable data protection legislation. This includes the General Data Protection Regulation (GDPR), the UK Data Protection Act, and any other relevant local or international laws and regulations pertaining to data protection and privacy.

GDPR Compliance

- Lawfulness, Fairness, and Transparency: We process personal data lawfully, fairly, and in a transparent manner, providing clear information about how data is used.
- Purpose Limitation: Data is collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.
- Data Minimisation: We ensure that the personal data we process is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
- Accuracy: We take every reasonable step to ensure that personal data is accurate and, where necessary, kept up to date.
- Storage Limitation: Personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- Integrity and Confidentiality: We process personal data in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

UK Data Protection Act

Kaizen Certification Ltd adheres to the principles and obligations set out in the UK Data Protection Act, ensuring that data processing activities align with UK-specific regulations and requirements.

Updates to Legislation

We regularly monitor legal developments and update our practices to remain compliant with changes in data protection laws.

Compliance with Legislation

Energy Performance of Buildings data and Register obligations

For England and Wales. Energy Performance of Buildings (EPB) assessment data collected under the EPB Regulations 2012 remains the intellectual property of MHCLG. including UPRN and

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

RRN issued by the Register. EPB data is used solely for producing and validating EPCs. DECs and ACIRs, and is stored only to support SOR compliance such as audits and complaints.

Kaizen will act as Data Controller for any assessment data it shares with an authorised person. or a third party with the authorised person's consent. and will operate a Data Sharing Plan that logs recipients. legal basis. security controls. incidents and an annual audit of sharing. We will provide the Plan and evidence on request to MHCLG or its auditors.

Assessment data means the calculation data. floor plans. photographs and documentation used to support the assessment and assumptions.

Scotland. Approved Organisation obligations

For Scottish EPCs lodged under the Energy Performance of Buildings (Scotland) Regulations 2008. Kaizen will operate to the Scottish Government Operational Framework for Approved Organisations. including. at minimum. maintaining auditable records for five years. publishing Code of Conduct. and supporting complaints. appeals and disciplinary processes. We will notify the keeper of the Scottish Register of any change in an assessor's membership status within one working day. and cooperate with Scottish Government audit.

Responsibility and Accountability

- Kaizen Certification Ltd takes responsibility for, and is able to demonstrate compliance with, the data protection principles.
- Our Data Protection Officer (DPO) oversees compliance and is the point of contact for data protection authorities.

Training and Awareness

- Regular training on data protection laws and regulations is provided to all staff to ensure that they understand their obligations and the importance of compliance.
- We maintain a culture of data protection awareness within the organisation.

Breach Notification

In the event of a data breach, we follow the legal requirements for notification to the relevant supervisory authorities and, where applicable, to the data subjects.

International Considerations

For international data transfers, we ensure compliance with legal requirements, providing adequate protection for the transfer of personal data outside the EEA.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

4. Principles of Data Handling

Commitment to Data Protection Principles

Kaizen Certification Ltd is committed to adhering to the core principles of data handling as outlined in the GDPR and the UK Data Protection Act. These principles guide our practices and ensure the responsible and lawful treatment of personal data.

Principles

- Lawfulness, Fairness, and Transparency:
  Data is processed lawfully, fairly, and in a transparent manner.
  Individuals are informed about how their data is being used, ensuring clarity and openness.
- Purpose Limitation:
  Data is collected for specified, explicit, and legitimate purposes.
  We avoid processing data for purposes that are not clearly outlined or compatible with the original purpose of collection.
- Data Minimisation:
  Only data that is necessary for the intended purposes is collected and processed.
  We regularly review our data collection practices to ensure that only relevant data is retained.
- Accuracy:
  We ensure the accuracy of personal data and keep it up to date.
  Inaccurate data is rectified or deleted without delay.
- Storage Limitation:
  Data is kept in a form that permits identification of data subjects only as long as necessary for the processing purposes.
  We implement policies and procedures for the regular review and deletion or anonymisation of data when it is no longer needed.
- Integrity and Confidentiality:
  Personal data is processed securely, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing, accidental loss, destruction, or damage.
  We foster a culture of security and confidentiality regarding personal data.
- Accountability:
  Kaizen Certification Ltd takes responsibility for the personal data we handle and demonstrates compliance with the above principles.
  We maintain records of processing activities and implement data protection policies, impact assessments, and regular audits to ensure ongoing compliance.

Implementation

- All employees and personnel who interact with personal data are trained and informed about these principles.
- Procedures and policies are regularly reviewed and updated to ensure they reflect these principles.

Data Subject Rights

We respect and facilitate the exercise of data subjects' rights under the GDPR, including the right to access, rectify, erase, restrict processing, data portability, object to processing, and rights related to automated decision-making and profiling.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

5. Data Security Measures

Overview

At Kaizen Certification Ltd, we recognise the importance of implementing robust data security measures to protect personal data against unauthorised access, alteration, disclosure, or destruction. Kaizen maintains Cyber Essentials Plus certification. The SORs require schemes to hold either ISO/IEC 27001 or Cyber Essentials Plus. Evidence of current certification is held and provided on request to MHCLG or its agents.

Technical Measures

- Data Encryption:
  Use of encryption technologies to protect data during transmission and while stored.
  Ensuring sensitive information is securely encrypted according to industry standards.
- Access Control:
  Strict access controls to ensure that only authorised personnel can access personal data.
  Use of passwords, two-factor authentication, and other security measures to prevent unauthorised access.
- Network Security:
  Implementation of firewalls, anti-virus software, and other network security measures.
  Regular updates and patches to our IT infrastructure to protect against vulnerabilities.
- Data Backup and Recovery:
  Regular backups of personal data to prevent loss.
  Robust data recovery procedures in place to restore data in case of a security breach or technical issue.
- Enhanced Cybersecurity Tools:
  Incorporate advanced cybersecurity technologies such as machine learning and AI-driven threat detection systems to enhance our capabilities in identifying and responding to security threats in real-time. These tools will augment our existing security measures by providing predictive analytics to prevent potential data breaches before they occur.

Organisational Measures

- Security Policies and Procedures:
  Clear and comprehensive security policies and procedures that are regularly reviewed and updated.
  Regular audits and assessments to ensure compliance with these policies.
- Staff Training and Awareness:
  Ongoing training for staff on data security and privacy principles.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

Awareness programs to keep staff informed about the latest security threats and prevention techniques.

- Data Breach Response Plan:
  A well-defined data breach response plan to ensure prompt and effective action in the event of a security breach.
  Procedures for notifying relevant authorities and data subjects in compliance with GDPR requirements.
- Vendor and Third-Party Management:
  Ensuring that all vendors and third parties who handle personal data on our behalf adhere to equivalent data security standards.
  Conducting regular reviews and audits of third-party service providers.

Monitoring and Evaluation

- Regular monitoring of our data security measures to ensure their effectiveness.
- Evaluating the impact of new technologies and business processes on data security.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

6. Data Sharing and Disclosure

Introduction

Kaizen Certification Ltd recognises that sharing and disclosing personal data are integral aspects of our operations. However, such activities are carried out with utmost regard for privacy and data protection laws. This section outlines our approach to data sharing and disclosure, ensuring compliance with legal and ethical standards.

For EPB assessment data. sharing is permitted only in line with the EPB Regulations and SORs. Kaizen will:

- share only with an authorised person or a third party with the authorised person's consent.
- apply approved transfer controls. encrypt data in transit and at rest. and prohibit secondary use.
- maintain a Data Sharing Plan with annual audit. logging each share. security applied. and any loss or unauthorised release.

Principles of Data Sharing and Disclosure

- Legitimate and Lawful Sharing: Data is only shared or disclosed for legitimate purposes, and in accordance with legal requirements. We ensure all data sharing aligns with the purposes for which the data was initially collected.
- Minimum Necessary Disclosure: We only disclose the minimum amount of data necessary for the intended purpose. When possible, data is anonymised or pseudonymised before sharing.
- Consent and Transparency: Where required, explicit consent is obtained before sharing personal data. Individuals are informed about the nature of the sharing, the parties involved, and the purpose of the disclosure.
- Data Sharing Agreements: Where data is shared with third parties, Data Sharing Agreements are in place to ensure that these parties adhere to the same standards of data protection as Kaizen Certification Ltd.

Data Sharing within the Organisation

- Internal Access Control: Access to personal data within the organisation is limited to those who need the information to perform their job responsibilities.
- Training and Awareness: Staff involved in data sharing are trained in data protection principles and understand the importance of confidentiality and privacy.

External Data Sharing

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

- Third-Party Processors: When using third-party processors, we ensure they comply with GDPR and provide sufficient guarantees regarding their data protection measures.
- Legal Obligations: In certain circumstances, we may be legally required to share data with law enforcement agencies, regulatory bodies, or as part of legal proceedings. Such sharing will be carried out in full compliance with legal procedures.

International Data Transfers

- Cross-Border Transfers: When transferring data outside the European Economic Area, we ensure appropriate safeguards are in place, such as Standard Contractual Clauses or adherence to international frameworks like the EU-US Privacy Shield.

Data Disclosure Practices

- Routine and Ad Hoc Disclosures: We maintain records of routine data disclosures and conduct assessments for any ad hoc requests to ensure compliance with our policy and legal obligations.
- Notification of Data Breaches: In the event of a data breach involving unauthorised disclosure, affected individuals will be notified in accordance with GDPR guidelines.

Review and Oversight

- Regular Audits: Data sharing and disclosure practices are regularly audited for compliance with this policy and relevant data protection laws.
- Continuous Improvement: We continually review and update our data sharing and disclosure practices to adapt to new legal requirements and best practices.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

7. Data Subject Rights

Overview

Under the GDPR and the UK Data Protection Act, individuals (data subjects) have specific rights concerning their personal data. Kaizen Certification Ltd is committed to facilitating the exercise of these rights in a transparent, efficient, and timely manner.

Rights of the Data Subject

- Right to Access:
  Individuals have the right to access their personal data and obtain a copy of it.
  Kaizen Certification Ltd will provide a response to access requests without undue delay and within one month of receipt of the request.
- Right to Rectification:
  Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.
  Corrections will be made promptly, ensuring data remains accurate and up-to-date.
- Right to Erasure ('Right to be Forgotten'):
  Individuals have the right to have personal data erased under certain circumstances, such as when the data is no longer necessary for the purpose it was collected, or consent is withdrawn.
  Kaizen Certification Ltd will assess each request for erasure individually and respond in accordance with legal obligations.
- Right to Restrict Processing:
  Individuals have the right to request the restriction of processing of their personal data in certain circumstances, such as when the accuracy of the data is contested or the processing is unlawful.
  During the period of restriction, data can be stored but not processed further.
- Right to Data Portability:
  Individuals have the right to receive the personal data they have provided to Kaizen Certification Ltd in a structured, commonly used, and machine-readable format. They also have the right to request that this data be transmitted to another controller.
  This right applies to personal data processed by automated means and based on consent or contractual necessity.
- Right to Object:
  Individuals have the right to object to the processing of their personal data in certain circumstances, including for direct marketing purposes.
  Upon receiving an objection, Kaizen Certification Ltd will cease processing unless there are compelling legitimate grounds for continued processing.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

- Rights in relation to Automated Decision Making and Profiling:
  Individuals have the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them.
  Kaizen Certification Ltd ensures transparency and fairness in any automated decision-making processes.

Exercising Rights

- Requests to exercise data subject rights can be made in writing or verbally.
- Kaizen Certification Ltd will provide information on the actions taken in response to a request without undue delay and in any event within one month of receipt of the request.
- Information will be provided free of charge, except in cases of unfounded or excessive requests, where a reasonable fee may be charged.

Contact and Complaints

- Data subjects can contact our Data Protection Officer (DPO) for all matters related to the processing of their personal data and the exercise of their rights.
- If data subjects are not satisfied with the response or handling of their request, they have the right to lodge a complaint with the Information Commissioner's Office (ICO).

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

8. Data Breach Response

Purpose

The Data Breach Response section of Kaizen Certification Ltd's Data Protection Policy outlines the procedures for responding to any breach of personal data. This policy ensures timely and effective handling of breaches to mitigate any potential harm.

Definition of a Data Breach

A data breach involves the unauthorised or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are accidental or deliberate.

Detection and Reporting

- Detection: All staff are trained to recognise and report data breaches promptly.
- Reporting Procedure: In the event of a data breach, staff must immediately report it to the designated Data Protection Officer (DPO).

Simulated Breach Drills

- Include regular simulated data breach drills to ensure that all team members are proficient in their roles during an actual data breach scenario. These drills will help in identifying any weaknesses in our response strategy and provide practical insights into improving our breach response times and effectiveness.

Assessment and Investigation

- Upon receiving a report of a breach, the DPO will conduct an initial assessment to determine the scope and impact of the breach.
- A detailed investigation will be initiated to understand the cause and extent of the breach.

Containment and Recovery

- Immediate steps will be taken to contain the breach and prevent further unauthorised data access or loss.
- Efforts will be made to recover any lost data and to secure compromised systems.

Notification

- Authorities: If the breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority (e.g., the Information Commissioner's Office in the UK) will be notified within 72 hours of the organisation becoming aware of it.
- Data Subjects: If the breach is likely to result in a high risk to the rights and freedoms of individuals, those affected will be notified directly without undue delay. Notification will

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

include the nature of the breach, contact points for more information, likely consequences, and measures taken or proposed to address the breach.

Documentation

- All data breaches will be documented, including the facts about the breach, its effects, and the remedial actions taken. This documentation will be used to assess patterns or areas for improvement in data protection practices.

Review and Evaluation

- Post-incident analysis will be conducted to evaluate the response and to implement lessons learned.
- Measures will be reviewed and updated where necessary to prevent future breaches.

Training and Awareness

- Regular training and awareness sessions on data breach response will be conducted for all staff.
- This training will include recognising the signs of a data breach, reporting procedures, and preventive measures.

Kaizen Certification Ltd's Data Breach Response policy is an integral part of our commitment to safeguarding personal data. Through prompt and effective handling of data breaches, we aim to uphold our responsibility to protect the data we manage and maintain the trust of our clients, employees, and stakeholders.

9. Training and Awareness

Purpose

The purpose of the Training and Awareness section in Kaizen Certification Ltd's Data Protection Policy is to ensure that all employees and relevant stakeholders are well-informed about their data protection responsibilities. This section emphasises the importance of continuous education and awareness in fostering a culture of data protection within the organisation.

Employee Training

- Regular Training Sessions: Conduct regular training sessions for all employees on data protection laws, regulations, and best practices. This includes GDPR and the UK Data Protection Act.
- Induction Training: New employees receive data protection training as part of their induction process to ensure immediate awareness of their responsibilities.
- Role-Specific Training: Provide specialised training for roles that handle significant amounts of personal data or that involve higher data protection risks.

Gamification in Training

- Integrate gamification techniques into our data protection training programs to increase engagement and retention of information. This approach will include interactive scenarios, challenges, and rewards that encourage active participation and ongoing learning among employees.

Awareness Programs

- Regular Updates: Disseminate regular updates on data protection matters, including changes in legislation, emerging risks, and best practices.
- Engagement Activities: Implement activities such as workshops, quizzes, and newsletters to keep data protection at the forefront of employees' minds.

Management and Leadership Training

- Leadership Role in Data Protection: Train management and leadership teams to understand their critical role in upholding data protection standards and leading by example.
- Decision-Making and Data Protection: Include data protection considerations in management and leadership training to ensure it is a key factor in decision-making processes.

Data Protection Officer (DPO) Role

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

- DPO Expertise: Ensure the Data Protection Officer is provided with the necessary resources and training to stay updated on data protection laws and practices.
- DPO Accessibility: Make the DPO accessible to all staff for advice and consultation on data protection matters.

Record Keeping

- Training Records: Maintain detailed records of all training sessions, including attendees, topics covered, and materials used.
- Feedback and Improvement: Collect feedback on training sessions and use it to continuously improve the training content and delivery methods.

Third-Party and Contractor Training

- Training for Third Parties: Ensure that third-party service providers and contractors who handle personal data on behalf of Kaizen Certification Ltd receive appropriate data protection training.
- Contractual Obligations: Include data protection training requirements in contracts with third parties to ensure consistency in data handling practices.

Kaizen Certification Ltd's commitment to Training and Awareness in data protection is integral to our overall data security strategy. By empowering our employees and relevant stakeholders with the knowledge and tools they need, we reinforce our commitment to safeguarding personal data and upholding the highest standards of privacy and security.

10. Record Retention and Disposal

Purpose

The Record Retention and Disposal section of Kaizen Certification Ltd's Data Protection Policy outlines our approach to retaining personal data only as long as necessary and ensuring its secure and appropriate disposal. This practice is crucial for maintaining data protection and privacy standards.

Record Retention

- Retention Periods:
  Personal data is retained only for as long as necessary for the purposes for which it was collected, including for the purposes of satisfying any legal, accounting, or reporting requirements.
  Retention periods are determined based on the nature of the data, the purpose of its use, and any applicable legal or regulatory requirements.
- Review of Data:
  Regular reviews are conducted to identify data that no longer needs to be retained.
  Automated systems may be used where feasible to manage data retention periods.
- Secure Storage During Retention:
  While retained, data is stored securely to prevent unauthorised access and ensure its integrity and confidentiality.

Retention schedule for EPB records

- Audit evidence supplied by members to Kaizen. retained only as long as necessary and not beyond 10 years from audit date. in line with Level 2 SORs.
- Assessor job evidence retained by the member. retained by the member for a minimum of 15 years. per Code of Conduct.
- Scottish AO minimum. Kaizen retains Scottish Operational Framework records for at least 5 years. which is met within the above 10-year Kaizen limit.

Data Disposal

- Secure Disposal Methods:
  When data is no longer needed, it is disposed of securely and effectively.
  Secure disposal methods include shredding of paper records and secure electronic deletion or destruction of digital data.
- Documentation of Disposal:
  Records of data disposal are maintained, documenting the type of data disposed of and the method and date of disposal.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

- Third-Party Disposal:
  If third parties are employed to dispose of data, they must provide guarantees of their compliance with GDPR and secure disposal methods.

Legal and Regulatory Compliance

- Compliance with legal and regulatory requirements governing record retention and disposal, including industry-specific requirements.
- Ensuring that data retention and disposal practices are consistent with data subject rights under GDPR.

Training and Awareness

- Staff are trained in the organisation's data retention and disposal procedures.
- Awareness is raised about the importance of proper data retention and secure disposal in protecting data subjects' privacy.

Review and Updating of Retention and Disposal Practices

- Regular review of data retention and disposal practices to ensure they remain appropriate and compliant with current laws and best practices.
- Updates to retention and disposal practices as necessary to reflect changes in legal requirements or operational needs.

Kaizen Certification Ltd's approach to record retention and disposal is designed to balance the need to retain data for operational, legal, and regulatory purposes with the obligation to dispose of data responsibly when it is no longer required. This careful management of data lifecycle is a key component of our commitment to responsible data handling and protection.

11. Policy Review and Updates

Commitment to Continual Improvement

Kaizen Certification Ltd is committed to the continuous improvement and updating of its Data Protection Policy. This commitment ensures that our practices not only comply with current legislation but also reflect the best practices in data protection and privacy.

Regular Policy Review

Scheduled Reviews: The Data Protection Policy is reviewed at regular intervals (at least annually) or when significant changes in data processing activities or data protection laws occur.

Stakeholder Involvement: Reviews include input from key stakeholders within the organisation, including management, the Data Protection Officer (DPO), IT personnel, and legal advisors.

Adapting to Changes

Regularly engage external stakeholders, including clients and partners, to provide feedback on our data protection practices. This feedback will be used to ensure our policy adjustments not only comply with legal standards but also align with the expectations and requirements of the people and organisations we serve.

Adapting to Changes

Legal and Technological Changes: The policy is updated to reflect changes in data protection legislation, technological advancements, and industry best practices.

Operational Changes: Adjustments are made to address changes within the organisation's structure, processes, or systems that impact data protection.

Documentation of Changes

Record of Amendments: A record of all changes made to the policy is maintained, including the date of the change and a summary of the amendments.

Version Control: The policy document includes version control to ensure clarity on the most current version.

Communication of Updates

Internal Communication: All updates to the policy are communicated to staff in a timely manner. This includes highlighting key changes and their impact on daily operations.

Training and Awareness: Following significant updates, additional training or awareness sessions are provided to ensure all employees understand the new requirements.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

Data Protection Officer (DPO) Role

DPO Oversight: The DPO is responsible for overseeing the review and update of the Data Protection Policy.

Guidance and Expertise: The DPO provides expert advice and guidance on data protection laws and practices to inform policy updates.

Feedback Mechanism

Staff Feedback: Staff feedback is encouraged and considered during policy reviews to incorporate practical insights and suggestions.

Continuous Improvement Loop: Feedback mechanisms are part of a continuous improvement loop, ensuring the policy remains effective and relevant.

External Consultation (where necessary)

Legal and Industry Experts: External consultation with legal experts and industry specialists may be sought to ensure comprehensive and compliant policy updates.

The regular review and updating of the Data Protection Policy ensure that Kaizen Certification Ltd remains at the forefront of data protection standards, adapting to new challenges and changes in the environment in which we operate. Our proactive approach to policy management is integral to maintaining the trust of our clients, employees, and stakeholders in our data protection practices.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

12. Compliance Monitoring and Auditing

Purpose

Kaizen Certification Ltd is committed to ensuring ongoing compliance with its Data Protection Policy. This section outlines our approach to monitoring and auditing these practices to maintain high standards of data protection and privacy.

Regular Compliance Monitoring

- Continuous Oversight: Regular monitoring of data processing activities to ensure they align with the Data Protection Policy.
- Role of the Data Protection Officer (DPO): The DPO is responsible for overseeing compliance monitoring, identifying areas of potential non-compliance, and recommending corrective actions.

Internal Auditing

- Scheduled Audits: Conducting periodic internal audits to assess compliance with data protection laws and policy guidelines.
- Audit Scope and Methodology: Audits cover all aspects of data handling, including collection, storage, processing, and sharing. Audits are conducted using established methodologies that ensure thoroughness and accuracy.

External Auditing

- Engagement of Independent Auditors: Where necessary, external auditors are engaged to provide an objective assessment of compliance with data protection regulations and the effectiveness of the Data Protection Policy.
- Audit Reports and Recommendations: External audit findings are documented in reports, which include recommendations for improvements.

Responding to Audit Findings

- Corrective Actions: Prompt implementation of corrective actions in response to audit findings.
- Follow-Up Audits: Conducting follow-up audits to ensure that corrective actions have been effective.

Reporting and Documentation

- Audit Records: Maintaining comprehensive records of all internal and external audits, including findings, recommendations, and actions taken.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd

- Reporting to Senior Management: Regular reporting of audit outcomes to senior management to ensure high-level oversight and accountability.

Employee Involvement and Feedback

- Staff Participation: Encouraging employee participation in the auditing process to foster a culture of compliance and transparency.
- Feedback Mechanisms: Implementing feedback mechanisms to gather insights from employees on data protection practices and potential areas for improvement.

Training and Awareness Post-Audits

- Training Programs: Updating training programs based on audit findings to address any identified gaps in knowledge or practice.
- Awareness Campaigns: Conducting awareness campaigns post-audits to highlight important findings and reinforce the importance of data protection.

Compliance with Changing Regulations

- Adaptability: Ensuring that monitoring and auditing practices are adaptable to changes in data protection laws and industry standards.

Kaizen Certification Ltd's commitment to compliance monitoring and auditing is a testament to our dedication to upholding the highest standards of data protection. Through these efforts, we ensure that our Data Protection Policy is not just a document, but a living framework that actively guides our operations and safeguards the data entrusted to us.

We will make our Data Sharing Plan. logs and audit outcomes available to MHCLG. the Register Operator. and the Scottish Government on request. and record corrective actions to closure.

Appendix A – Data Sharing Plan (SOR 1.2.13)

Kaizen keeps a live log of every data release (date / recipient / lawful basis). The log is audited annually and a summary report is supplied to MHCLG upon request. Any loss or unauthorised release is reported to ICO and MHCLG within 72 hours.

hello@Kaizencertification.co.uk | © Kaizen Certification Ltd