

Data Sharing Plan Excerpts & Data Controller Duties

1. Introduction

This document outlines Kaizen Certification Ltd's approach to data sharing, Data Controller responsibilities, and GDPR compliance in accordance with Level 1 SORs

§1.2 (vi) and Level 2 SORs §1.5/§4.5. It provides essential information for prospective members regarding data protection obligations and assessment data sharing procedures.

2. Data Controller Status & Responsibilities

2.1 When Kaizen Becomes a Data Controller

Kaizen Certification Ltd becomes a Data Controller for 'assessment data' when:

- Assessment data is shared with building owners, landlords, or occupiers
- Assessment data is shared with third parties with consent of authorized persons
- Data sharing activities fall under the Energy Performance of Buildings Regulations 2012 (as amended)

2.2 Assessment Data Definition

Assessment data includes:

- Energy calculation data
- Floor plans and photographs
- Any documentation supporting data entry
- Assumptions made during the assessment process
- Evidence gathered during site visits

2.3 Data Controller Obligations

As a Data Controller, Kaizen Certification Ltd must:

- Comply with UK General Data Protection Regulation (UK GDPR)
- Comply with Energy Performance of Buildings Regulations 2012 (as amended)
- Implement appropriate technical and organizational measures
- Report non-compliance to MHCLG and appropriate authorities
- Maintain records of all data sharing activities

3. Data Sharing Procedures

3.1 Authorized Data Sharing

Assessment data may only be shared with:

- Building owners (authorized persons)

- Landlords (authorized persons)
- Occupiers (authorized persons)
- Third parties with explicit consent from authorized persons

3.2 Prohibited Data Sharing

Assessment data must NOT include:

- Green Deal information
- Names of individuals (including Energy Assessor, homeowner, or any identifying individual names)
- Assessment data relating to 'excluded buildings' (military buildings or other excluded buildings as defined in EPB Regulations)

3.3 Data Sharing Controls

- All data sharing must use controls approved by Kaizen Certification Ltd
- Recipients must understand and accept UK GDPR requirements
- Data sharing must comply with EPB Regulations and Data Protection legislation
- Written consent required from authorized persons for third-party sharing

4. Data Protection Management

4.1 Lawful Basis for Processing

Data processing under this scheme relies on:

- Legal obligation - Compliance with EPB Regulations 2012
- Legitimate interests - Energy efficiency improvement purposes
- Consent - Where explicit consent obtained for third-party sharing

4.2 Data Subject Rights

Under UK GDPR, data subjects have rights to:

- Access their personal data
- Rectification of inaccurate data
- Erasure in certain circumstances
- Restriction of processing
- Data portability where applicable
- Object to processing in certain circumstances

4.3 Data Retention Periods

- Assessment data: Retained as long as necessary for compliance purposes
- Audit evidence: Maximum 10 years from audit date
- Member records: 15 years minimum as per SOR requirements

- Audit outcomes: May be retained beyond 10 years for compliance

5. Data Security Measures

5.1 Technical Safeguards

- Secure storage on internal servers with restricted IP access
- HTTPS protocols for all data transmission
- Web authentication and validation processes
- Separate audit system isolated from main systems
- Regular security assessments and updates

5.2 Organizational Measures

- Staff training on data protection principles
- Access controls based on role requirements
- Regular audits of data handling procedures
- Incident response procedures for data breaches
- Data Protection Officer appointed and available

5.3 Data Sharing Security

- Encryption of data in transit and at rest where appropriate
- Secure transfer methods for assessment data sharing
- Audit trails of all data sharing activities
- Recipient verification before data release

6. Monitoring & Reporting Procedures

6.1 Data Sharing Activity Monitoring

Kaizen Certification Ltd maintains records of:

- When assessment data is shared
- Who receives the data (authorized persons or third parties)
- What data is shared
- Legal basis for sharing
- Consent evidence where applicable

6.2 Annual Audit Requirements

- Minimum annual audit of data sharing activities
- Verification that UK GDPR accepted by data recipients
- Review of data sharing controls and procedures
- Assessment of data security measures
- Reporting to MHCLG on data sharing compliance

6.3 Non-Compliance Reporting

Kaizen Certification Ltd will report to appropriate authorities:

- Data breaches affecting assessment data
- Unauthorized data sharing incidents
- Member non-compliance with data sharing rules
- System security incidents or vulnerabilities

7. Member Responsibilities

7.1 Data Collection Obligations

Energy Assessors must:

- Collect data lawfully and transparently
- Inform building occupants of assessment purpose and data use
- Obtain necessary permissions for photographs and data collection
- Use only approved software and data collection methods
- Store data securely for minimum 15 years

7.2 Data Sharing Compliance

Members must:

- Only share data through approved Kaizen Certification Ltd controls
- Verify recipient authorization before sharing
- Obtain appropriate consents for third-party sharing
- Report data incidents to Kaizen Certification Ltd immediately
- Comply with scheme data sharing procedures

7.3 Prohibited Activities

Members must NOT:

- Store data longer than necessary in non-compliant systems
- Share data without legitimate reason or proper consent
- Disclose data in ways non-compliant with EPB Regulations
- Use assessment data for purposes other than energy efficiency improvement

8. GDPR Compliance Framework

8.1 Data Protection by Design

- Privacy considerations built into all processes
- Minimal data collection - only what's necessary

- Purpose limitation - data used only for stated purposes
- Accuracy requirements - data kept up to date and correct
- Storage limitation - data not kept longer than necessary

8.2 Transparency Measures

- Clear communication about data use to building occupiers
- Privacy notices available and accessible
- Data subject rights clearly explained
- Contact information provided for data protection queries
- Regular updates on data protection practices

8.3 Accountability Measures

- Written procedures for all data processing activities
- Regular training for staff and members
- Documentation of compliance measures
- Regular reviews of data protection practices
- External audits where appropriate

9. Contact Information

9.1 Data Protection Officer

Kaizen Certification Ltd Data Protection Officer

Email: dpo@kaizencertification.co.uk

9.2 General Data Protection Queries

Customer Services

Email: hello@kaizencertification.co.uk Phone: 0330 223 6278

Address: Bishops Court, 17a The Broadway, Hatfield, Hertfordshire AL9 5HZ

9.3 Data Subject Rights Requests

For exercising data subject rights, please contact: Email:
dataprotection@kaizencertification.co.uk

Or write to the address above marking correspondence "Data Subject Rights Request"

10. Regulatory References

10.1 Key Legislation

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

- Energy Performance of Buildings (England and Wales) Regulations 2012 (as amended)
- Privacy and Electronic Communications Regulations

10.2 Regulatory Authorities

- Information Commissioner's Office (ICO) - Data protection supervision
- Ministry of Housing, Communities and Local Government (MHCLG) - EPB compliance
- Energy Assessor Scheme Operating Board (EASOB) - Industry standards

SOR data-sharing controls

Members who share assessment data outside Kaizen-approved controls are subject to disciplinary action and, where required, reporting to MHCLG and other authorities. Recipients must accept UK GDPR and relevant data protection obligations before assessment data is released.