



SLH Data Scrutiny Review Report, December 2024



Summary

In November 2024, a scrutiny group of customers met to evaluate SLH's data protection, which also covered data security and 'Access to Information' in preparation for the upcoming new Consumer Standard. The group approved the final report in January 2025.

Overall, the customers concluded that SLH has robust policies and procedures for data protection, including handling Data Subject Access Requests (DSARs), data breaches, and cybersecurity threats.

Identified areas for improvement included;

- Reducing the number of data breaches caused by staff emailing information to the wrong person.
- Ensuring that SLH can manage data security incidents out of office hours, where the threat levels are higher, and the impact can be far more reaching if SLH is slow to respond.
- Forming a working group of residents to oversee how SLH implements the new Access to Information process.

SLH colleagues advised that investment in data protection and data security training continues to be reviewed and enhanced. The 2025/26 budget setting process will also consider additional cyber defence tools including Email Encryption and a 24-hour Managed Detection Response service. This will be considered alongside other demands on the budget.

The Scrutiny group conducted a review of SLH's compliance with the Data Protection Act 2018 and preparation for the new Consumer Standard, including;

Data Protection

- Overview of legislative and regulatory requirements.
- Desktop review of what tenant data SLH holds, how it is stored and controls around how it is accessed.
- Review of how long data and records are kept, and how it is deleted.
- Desktop review of the process for dealing with requests i.e., data subject access requests and compliance with timescales for responding.

Data Security

- Reviewing the current cyber security threats and what this may mean for security of tenant's personal data, including threats associated with Artificial Intelligence Tools.
- Undertaking a 'deep dive' into the My Account application.
- Noting independent sources of assurance e.g., audit reports, systems testing, certification.

Access to Information – preparation for the forthcoming new Consumer Standard

- Social Tenants Access to Information Requirements scheme.
- Review plans for improving access to information available on the Website.

Members sought to answer the following questions

1. What are customers' rights under data protection legislation and how does SLH ensure that the legislation is followed?
2. How is customer data shared with contractors and what measures are in place to protect the data?
3. How does SLH manage Data Subject Access requests?
4. What is the most common data breach at SLH and how does SLH manage data breaches?
5. How secure is SLH customer personal data?
6. How are SLH colleagues trained in data protection?
7. How is data held in MyAccount and is it secure?
8. What Information can be added to the SLH website to support Tenants in understanding their rights in line with the Social Tenants to Access Information Scheme?
9. Can SLH provide Information in accessible easy to easy-to-understand formats?

1. What are customers' rights under data protection legislation and how does SLH ensure that the legislation is followed?

Finding

Under data protection legislation, such as the General Data Protection Regulation (GDPR) in the EU and the Data Protection Act 2018 in the UK, customers have several key rights regarding their personal data

1. **Right to be informed:** Customers must be informed about how their data is being used.
2. **Right of access:** Customers can request access to their personal data.
3. **Right to rectification:** Customers can request corrections to inaccurate or incomplete data.
4. **Right to erasure:** Also known as the "right to be forgotten," customers can request the deletion of their data.
5. **Right to restrict processing:** Customers can request the restriction of their data processing.
6. **Right to data portability:** Customers can request their data be transferred to another service provider.
7. **Right to object:** Customers can object to the processing of their data.
8. **Rights related to automated decision-making and profiling:** Customers can request human intervention in automated decisions.

1. What are customers' rights under data protection legislation and how does SLH ensure that the legislation is followed?

Finding

SLH ensures compliance with these regulations through several measures including;

- **Information Governance:** SLH has a structured approach to managing data protection, including appointing a Data Protection Officer (DPO) and Information Security Officer (ISO) and implementing policies for data handling and data breaches.
- **Collection Handling and Use:** SLH collects only necessary data and uses it transparently for specified purposes, such as understanding customer vulnerabilities to meet their needs.
- **IT Controls and Security:** SLH employs technical and organisational measures to protect personal data from unauthorised access, loss, or damage.
- **Handling Subject Access Requests:** SLH has procedures in place to handle requests related to data access, correction, deletion, and other rights. These steps help ensure that SLH adheres to data protection laws and safeguards customer data effectively.
- A copy of the data protection and data privacy policy can be found on SLH website [here](#)

2. How is customer data shared with contractors and what measures are in place to protect the data?

Finding

- SLH can share individual personal data with third parties if this is essential to carrying out our legal responsibilities or protecting a customer from harm.
- SLH is legally responsible for its own breaches or breaches caused by the actions (or inactions) of data processors.
- Personal data passed to other organisations, or third parties is tightly controlled. SLH ensures that a contract is in place to ensure companies have adequate technical and organisational security measures in place to ensure that the risk of any data breach is minimised. 'Data Sharing Agreements' (for regular sharing) and / or appropriate sections in contracts with external contractors that allow access to the organisation's information systems must be in operation before access is allowed. The agreements/contracts ensure that the staff or sub-contractors of the external organisation comply with all appropriate SLH security policies. This will include examples including external researchers, insurers, maintenance contractors, debt collection agencies, auditors, and managing agents.
- SLH has Data Sharing Agreements in place and maintains a Data Sharing Register. SLH keeps its Privacy Notice page updated on the SLH website with changes to its data sharing and data protection policy. This advises customers and third parties who or why data is shared.

3. How does SLH manage Data Subject Access requests?

Finding

- Individuals have the right to information to be supplied within 30 calendar days. Once a request is received it is recorded within Cx which then automates a notification to the Data Protection Officer (DPO), Information Security Officer (ISO), and the Governance compliance coordinator. An acknowledgement of receipt is sent to the customer to confirm that SLH is managing the request. The customer's Identity is verified before efforts are made to locate and collate the customer data. If the data has third-party information enclosed, it needs to be redacted before being sent securely with a response.
- In line with SLH's procedure for handling information requests, the subject access request will be held on file for 6 months before being deleted.

Rights

- Right to information and transparency
- Right of access
- Right to object to processing (the right to say 'no and stop')
- Right to object to direct marketing
- Right not to be subject to automated decision making
- Right to data portability
- Right to the restriction of processing
- Right to correction/erasure of data (Right to be forgotten)
- Right to withdraw consent
- Right to complain
- Right to compensation

4. What is the most common data breach at SLH and how does SLH manage data breaches?

Finding

- The most common data breach is sending an email to the wrong recipient (around 8 times in a typical year). SLH has reviewed each data breach and completed a risk assessment. As a result of this type of data breach, SLH has removed the action of auto-populating names in email addresses to prevent this from happening.
- SLH uses the following steps to effectively manage the data breach and minimise the impact on customers and SLH as an organisation.
 1. Identify and Confirm the breach log in the Cx management system and or report to Service Desk for IT support
 2. Contain the breach
 3. Preserve evidence
 4. Notify relevant parties
 5. Conduct a thorough Investigation
 6. Remediate and Recover
 7. Review policies and Procedures
- Following the above actions SLH will then review lessons learnt and implement any additional control measures to prevent the breach from happening again in the future.

5. How secure is SLH customer personal data?

Finding

Customers noted the SLH cyber security policy ensuring compliance with the Data Protection Act 2018 and the Computer Misuse Act 1990. Tools SLH uses to ensure customer data is secure include:

- Internal & External Penetration Testing
- Continuous Vulnerability Scanning
- Payment Card Scanning
- Phishing simulations
- Darktrace email security reports
- Multi Factor Authentication on applications
- Microsoft Office CIS Security
- Cyber Essentials
- Internal Audit Reviews
- Staff training

6. How are SLH colleagues trained in data protection?

Finding

- Colleagues' complete data protection and cyber security face-to-face training with the ISO within 3 months of starting at SLH.
- SLH Colleagues must complete several online training courses which take place annually they include;
 - Encouraging a secure culture
 - Handling Sensitive Information
 - Password Security
 - Using the web safely
 - Social engineering
 - Artificial Intelligence Guidance
 - Phishing don't take the bait
- In addition to these courses, SLH conducts regular phishing email tests to assess our colleagues' knowledge and understanding. If a colleague clicks on a phishing email, they are required to retake the relevant training.
- SLH promotes a culture of vigilance and encourages colleagues to report any phishing emails. We also encourage colleagues to report any suspicious activity and anything that may compromise SLH's data security so that it can be investigated and stopped at the earliest opportunity.

7. How is data held in MyAccount and is it secure?

Finding

- My Account is a front-end web-based application for customers to self-serve. By design, the portal only shows relevant data to the customer and all data is stored in SLH's central system 'Civica Cx'. Customers can sign into the application using an email address and password. The password must meet standard security complexity along with a secret password.
- If the customer forgets their password, then they can reset it by sending a link to their email address to enter a new password along with confirming their secret password whilst completing the captcha code.
- The system is externally scanned every week using a web application testing piece of software (Currently Tenable.IO) which alerts SLH's security team to investigate any high severity alerts.

8. What Information can be added to the SLH website to support Tenants in understanding their rights in line with the Social Tenants to Access Information Scheme?

Finding

- Following the consultation by the Government ,the Regulator of Social Housing (RSH) will issue a new Access to Information Standard, possibly as early as April 2025. Under the plans, information can be requested for free by a tenant or their representative, such as a solicitor.
- Responding to information requests (people/process/system), with 30-day reporting.
- Dealing with complaints about the handling of requests (Housing Ombudsman).
- Providing information on the website, including publication of Frequently Asked Questions (anonymous).
- Registered providers must publish certain information about their activities and provide relevant information in response to requests from tenants unless it is reasonable to withhold the information from disclosure. In doing this, registered providers should demonstrate a commitment to transparency, accountability, and customer involvement.

9. Can SLH provide information in accessible, easy-to-understand formats?

Finding

- SLH has committed to providing and sharing information in easy-to-understand formats. SLH is using Mary Gobar International (MGI) to help with updating the website and ensuring the language used is customer-friendly and the website is easy to navigate.
- A local digital design agency has been employed to redesign the current SLH website from the ground up based on User Centric Design. Colleagues and customers have been involved in the design & testing process. Proposed launch Jan 2025. The website has intelligent search functionality and a Customer Information Hub, as well as compliant accessibility functionality to cater for a wide range of customer needs.

3 recommendations were identified by the scrutiny group, in addition to the ‘continue to’ recommendations on the next page.

1.Enhance Communication on Data Security Measures:

- Clearly articulate the extensive measures SLH takes to ensure data security, emphasising the safety and confidentiality of customer information.
- Highlight the comprehensive in-house training programs for staff, detailing how these programs ensure all colleagues understand their responsibilities and obligations regarding data protection.

2.Produce Data Security Awareness:

- Facilitate awareness/ information campaigns to educate customers about cybersecurity, helping them understand the importance of data protection and how they can contribute to it.
- Consider holding awareness sessions in sheltered schemes.

3. Involve Customers in Website Design:

- Engage customers in the design process of the Access to Information section on the SLH website, ensuring it meets their needs and is customer-centric.
- Form an Access to Information working group of customers to establish SLH’s Access to Information Scheme, monitoring requests for information and SLH’s performance.
- Produce a Privacy Impact Assessment for the new website.



Our Commitment to Continuous Improvement

- Review and update policies and procedures to reflect changes in Regulation and emerging threats.
- Regularly report and monitor data breaches and threats to the SLH Audit and Risk Committee.
- Share updates, learning and findings with customers concerning data breaches and data subject access requests.
- Implement ongoing training programs to keep colleagues informed about the latest data protection practices and emerging threats. Regularly update training to reflect new policies and technologies.
- Continuously monitor data access and usage through automated tools. Conduct regular audits to ensure compliance with data protection policies and to detect any breaches.
- Conduct regular incident response drills to test the effectiveness of SLH's Disaster Recovery plan. This will help to identify gaps and improve the response process.
- Establish feedback mechanisms where colleagues and customers can report issues or suggest improvements. Use this feedback to make enhancements to data protection measures.
- Regularly update and patch software and systems to protect against known vulnerabilities. Invest in new technologies that enhance data security, such as advanced encryption methods and intrusion detection systems.
- Foster a culture of continuous improvement by encouraging all colleagues to take ownership of data protection. Promote regular discussions on data security and recognise contributions that enhance data protection practices



Panel Membership

Scrutiny Panel members;

- SC
- GE
- CB
- LP
- HS
- PA
- LB

SLH colleagues;

- Emma Wilson, Governance & Compliance Co-ordinator
- Paul Aitken, Systems & Change Lead
- Hilary Tooke, Communications & Marketing Partner
- Lauren Crawford, Customer Engagement Partner
- John Mansergh, Director of Business Improvement