Data Breach Response Policy

Lilac ALLIANCE

Restraint Reduction Network

disability confident COMMITTED

Living Wage Employer

Bank House, Marshall Terrace, Crossgates Leeds LS15 8EA
0113 322 3765 contact@lilacalliance.co.uk

Data Breach Response Policy for Lilac Alliance in Compliance with GDPR and Data Protection Legislation

1. Introduction:

The General Data Protection Regulation (GDPR) imposes a duty on all organizations to report certain types of personal data breaches to the relevant supervisory authority. Lilac Alliance is required to do this within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we are also obligated to inform those individuals without undue delay. Lilac Alliance ensures that it has robust breach detection, investigation, and internal reporting procedures in place to facilitate decision-making about notification to the supervisory authority and affected individuals. Lilac Alliance is required to keep a record of all personal data breaches, regardless of the need for notification.

2. Scope:

This policy pertains to all personal data held by Lilac Alliance and data held on our behalf by nominated third-party providers and processors. Other relevant Lilac Alliance documents and policies include:

- Breaches log
- Breaches process flow
- Data processing addendum

3. Definitions:

Personal data breaches, as defined by the Information Commissioner's Office (ICO), encompass the following:

- Unauthorised third-party access
- Deliberate or accidental actions (or inactions) by a controller or processor
- Sending personal data to an incorrect recipient
- Loss or theft of computing devices containing personal data
- Unauthorized alteration of personal data
- Loss of availability of personal data

A data breach occurs when personal data is lost, destroyed, corrupted, disclosed, accessed, or passed on without proper authorization, or when data becomes unavailable (e.g., due to encryption by ransomware or accidental loss). When such a breach occurs, and Lilac Alliance becomes aware of it, the breaches procedure will be followed.

4. Responsibilities:

The Directors hold ultimate responsibility for managing data breaches and, if required, escalating them to relevant third-party providers and the ICO. The Data Protection Officer and IT Manager have specific responsibilities for preventing, managing, and recording data breaches. All staff are required to take reasonable steps to prevent data breaches and to be aware of the procedures to follow in the event of a data security breach.

5. Preparing for a Personal Data Breach:

5.1 Recognising a Breach:

All staff have been trained on what constitutes a personal data breach, including the definitions provided. Personal data breaches encompass loss, theft, unauthorized access, alteration, and unavailability of personal data. We have informed our customers that we will notify them of potential breaches promptly.

5.2 What to Do in the Event of a Personal Data Breach:

Lilac Alliance has a process flow explaining the actions required when a breach is identified. All staff are responsible for alerting relevant personnel if they are involved in a breach or become aware of one.

5.3 Responsibility for Managing Breaches:

The Data Protection Officer and IT Manager are initially responsible for managing data breaches. Senior staff members will be involved as necessary. When a breach affects data processed on behalf of another organization, Lilac Alliance will ensure that the Data Controller is informed, following Article 33(2) of the GDPR.

6. Responding to a Personal Data Breach:

6.1 Assessing the Likely Risk to Individuals:

The Data Protection Officer and IT Manager will assess the impact of the breach on individuals, and this assessment will be documented in the Data Breaches log.

6.2 Notifying the ICO of a Breach:

Lilac Alliance will notify the ICO within 72 hours when there is a likely risk to individuals' rights and freedoms. We will document our decision when we assess the risk.

6.3 Informing Affected Individuals About a Breach:

Lilac Alliance will contact affected individuals promptly, explaining the details of the breach and providing guidance to protect their information. For Data Controllers for whom Lilac Alliance processes data, we will make direct contact by email. For customers for whom Lilac Alliance acts as a Data Processor, we will liaise with the Data Controller to relay the necessary information as quickly as possible.

7. Documenting Breaches and Remedial Action:

Lilac Alliance will log all data breaches, documenting the facts, effects, and remedial actions taken, as required by Article 33(5) of the GDPR. Investigations will be conducted, and actions will be documented to prevent recurrence and inform corrective steps or further training.

Policy created 21.05.2023.
Review date 21.05.2026

Information Transfer and Communications Policy

1.0 Purpose

1.1 The purpose of this policy is ensuring that correct treatment when transferring information internally and externally to the company and to protect the transfer of information using all types of communication facilities.

2.0 Scope

- 2.1 All company employees and external party users.
- 2.2 Information that forms part of systems and applications deemed in scope by our Information Security Policy.

2.3 Company networks permitted for information transfer are out of scope for this document. Please see Access Control Policy.

3.0 Information Transfer Policy

3.1 Principles

- 3.1.1 Data transfer must comply with all legal and regulation legislation requirements including but not limited to the GDPR and Data Protection Act 2018.
- 3.1.2 Formal agreements that include non-disclosure and confidentially clauses must be in place for data sharing prior to the data transfer.
- 3.1.3 Personal data must not be transferred outside the European Economic Area without legal consent, justification, and legal mechanisms in place.
- 3.1.4 No personal or confidential information is to be transferred unencrypted.
- 3.1.5 All transfers are in line with IS 03 Information Classification and Handling Policy

3.2 Information Virus Checking

3.2.1 Information that is transferred is virus checked before being sent or before being opened when received.

3.3 Information Encryption

- 3.3.1 Personal and confidential information is always encrypted before being transferred.
- 3.3.2 Encryption credentials for username and password where used are shared via two separate and distinct communication methods. The preferred method is to share the username via email and the password via a voice call.

4.0 Data Transfer Methods

4.1 Preferred Transfer Method

4.1.1 The preferred transfer method is via Microsoft SharePoint or OneDrive. All users are licenced to store and share files using these systems.

SharePoint or OneDrive both allow files to be shared without sending a copy of the information directly. It also allows users to revoke or change permissions at any point.

- 4.1.2 When sharing information outside of Lilac Alliance, files will be stored within the appropriate SharePoint site.
- 4.1.3 When the data is no longer required to be shared, it is the responsibility of the sharer to revoke the access link.
- 4.1.4 When sharing information, a note should be added containing clear instructions of the recipient's responsibilities and instructions on what to do if they are not the correct recipient.

4.2 Data Transfer by Email

4.2.1 Email is never the best solution for transferring information as it is not secure and is not a guaranteed delivery mechanism. Consideration is always given to an alternative secure method of transferring sensitive data wherever possible and practicable.

- 4.2.2 Email communication should not be used to transfer unencrypted personal or confidential information.
- 4.2.3 Email messages must contain clear instructions of the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
- 4.2.4 Care must be taken as to what information is placed in the subject line of the email or in the accompanying message. Filename or subject line must not reveal the full contents of attachments or disclose any sensitive personal data.
- 4.2.5 The use of a personal email account is not permitted.

4.3 Data transfers by post/courier

4.3.1 Data transfers which occur via physical media such as paper reports, memory cards or CDs must only be dispatched an approved secure courier with a record of collection and a signature obtained upon delivery.

- 4.3.2 The recipient should be clearly stated on the parcel and the physical media must be securely packaged so that it does not break or crack.
- 4.3.3 The recipient should be advised in advance that the information is being sent so that they are aware when to expect the information. The recipient must confirm safe receipt as soon as the information arrives. The sender responsible for sending the data is responsible for confirming the data has arrived safely.

4.4 Data transfers on removable media / memory sticks

4.4.1 Removable media such as USB, memory sticks are not approved as a communication method for unencrypted confidential, personal, or otherwise sensitive data.

4.4.2 In exceptional circumstances and with IT approval, only company owned removable media is to be used for transferring information in line with policy the device usage is approved, recorded in the asset register, assigned, and encrypted.

- 4.4.3 The removable media must be returned to the owner on completion of the transfer and the transferred data must be securely erased from the storage device after use. The asset register must be updated.
- 4.4.4 Clear instructions of the recipient's responsibilities and instructions on what to do if they are not the intended recipient must be given.

- 4.4.5 Any accompanying message or filename must not reveal the contents of the media.
- 4.4.6 The removable media device must be encrypted.
- 4.4.7 The process described for Data transfers by post / courier must be followed.

4.5 Telephones, Mobile Phones and General Conversations

4.5.1 As phone calls may be monitored, overheard, or intercepted (either deliberately or accidentally), care must be taken as follows:

- 4.5.2 Be conscious of your surroundings especially on public transport such as trains and public places such as coffee shops when discussing personal, confidential, or otherwise sensitive information.
- 4.5.3 Personal data must not be transferred or discussed over the telephone unless you have confirmed the identity and authorisation of the recipient.
- 4.5.4 When using answer phones do not leave sensitive or confidential messages or include any personal data. Only provide a means of contact and wait for the recipient to speak to you personally.
- 4.5.5 When listening to answer phone messages left for yourself, ensure you do not play them in open plan areas which risks others overhearing. Delete them immediately after listening.
- 4.5.6 SMS must not be used to transfer confidential or private information. Encrypted email, Teams or another communication method must be used. SMS is not an encrypted system.

4.6 Data Transfers over Bluetooth

4.6.1 Bluetooth is not approved as a communication method for unencrypted confidential, personal, or otherwise sensitive data.

- 4.6.2 Ensure device mutual authentication is performed for all accesses.
- 4.6.3 Enable encryption for all broadcast transmissions (Encryption Mode 3).
- 4.6.4 Configure encryption key sizes to the maximum allowable.
- 4.6.5a Establish a —minimum key size for any key negotiation process. Keys should be at least 128 bits long

4.6.5b For Bluetooth: Use application-level (on top of the Bluetooth stack) authentication and encryption for sensitive data communication such as SSL.

- 4.6.7 Perform pairing as infrequently as possible, ideally in a secure area where attackers cannot realistically observe the passkey entry and intercept Bluetooth pairing messages.
- 4.6.8 Note: A “secure area” is defined as a non-public area that is indoors away from windows in locations with physical access controls.
- 4.6.9 Users should not respond to any messages requesting a PIN, unless the user has initiated a pairing and is certain the PIN request is being sent by one of the users ‘s devices.
- 4.6.10 Use only Security Mode 3 and 4. Modes 1 and 2 should not be allowed. Security Mode 3 is preferred but v.2.1 devices cannot use Security Mode 3.
- 4.6.11 Users should not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, or images.
- 4.6.12 All Bluetooth profiles except for Serial Port Profile should be always disabled, and the user should not be able to enable them.

4.7 Lost or missing information

4.7.1 If it is discovered or suspected that information has been lost, is missing, did not arrive, or has gone to the wrong person then the employee or external party user is required to inform at least one of their line manager, the information security management team, the management review team or the senior management team immediately at which point the company Breach Notification Process will be followed.

Policy Compliance

Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.

Other documents attached to this policy:

- Access controls
- Information classification (and handling)
- Asset register
- Acceptable use of assets
- Information Transfer And Communications Security Policy
- Physical Security Policy
- BYOD Policy
- GDPR and data protection policies

Policy created 21.05.2023.
Review date 21.05.2026

Information Governance and Data Security Training for Lilac Alliance and Sub-contractors:

Lilac Alliance recognises the critical importance of Information Governance (IG) and Data Security in ensuring the confidentiality, integrity, and availability of sensitive data. To uphold the highest standards of IG and Data Security, we have implemented a comprehensive training program for our staff and sub-contractors. Here are the key components of our training program:

1. Training Content and Curriculum:

- Our IG and Data Security training covers a wide range of topics, including but not limited to:
- GDPR (General Data Protection Regulation) compliance.
- Handling and safeguarding of sensitive and personal data.
- Cybersecurity best practices, including recognizing and mitigating security threats.
- Legal and ethical obligations related to information governance.
- Incident reporting procedures for data breaches or security incidents.

2. Training Frequency:

- All staff members and sub-contractors undergo IG and Data Security training upon onboarding.
- Annual refresher training is provided to ensure that all personnel remain up to date with the latest regulations and best practices.
- Additional ad-hoc training is conducted as needed in response to emerging threats or changes in data protection regulations.

3. Training Completion Assurance:

- We employ a robust system to track and ensure completion of IG and Data Security training by all staff.
- This includes maintaining detailed records of training attendance and completion certificates.
- Non-compliance is addressed promptly through our internal processes, which may include additional training and follow-up to ensure full understanding and compliance.

Training Figures for the Last Financial Year:

- In the last financial year, Lilac Alliance provided IG and Data Security training to 100% of our staff we do not utilise sub-contractors, if we did, we would ensure had same training as our own staff.
- We achieved a 100% completion rate for both initial onboarding training and annual refresher training.
- A total of 65 personnel participated in IG training during the last financial year.

IG Training Needs Analysis:

- Lilac Alliance conducts regular IG training needs analyses to identify gaps in knowledge and skills among our staff.
- This analysis is used to tailor our training programs to address specific areas of concern or emerging risks.
- The training needs analysis helps ensure that our training programs remain relevant and effective in maintaining the highest standards of IG and Data Security.

Lilac Alliance is committed to maintaining the confidentiality and security of all information we handle. Our robust IG and Data Security training program, with a proven track record of high completion rates, ensures that our staff are well-equipped to safeguard data and comply with relevant regulations, including GDPR.

Policy created 21.05.2023.
Review date 21.05.2026