Breach Notification Procedure

BS 10012:2017

Personal Information Management System		Scope	All LB Staff
Classification	Internal Use	Issue Date	November 2023
Lead Person	Data Protection Officer	Revision	3.0
Approval Committee	Company Directors	Review Date	November 2025

This policy is not contractual and can be reviewed, amended or withdrawn at any time.

Please be advised that Lothian Buses discourages the retention of hard copies of policies and procedures and can only guarantee that the policy on Lothian Buses' Intranet is the most up to date version.

Nick Connor

Data Protection Officer

1 CONTENTS

2 INTRODUCTION

At Lothian Buses, we believe that Personal Data Protection is a business enabler and shall not be seen as a constraint or cost. Appropriate Data Protection and Information Security policies have been implemented in a way that will allow the relevant information to be communicated clearly and allow the reader to develop their knowledge further by having more specific policies.

The Personal Data Protection policy framework at Lothian Buses is structured across three levels:

- The Computer Usage and Information Security Policy describing Lothian Buses's general principles and guidelines
- Operational Policies addressing Personal Data Protection topics in practical detail
- Significant topics of Data Protection regulation and procedures focusing on compliance

This approach combines both a comprehensive and practical way to describe how Personal Data Protection is handled at Lothian Buses and how individuals reach these objectives.

With this policy, Lothian Buses chooses to adopt a "risk driven strategy" as allowed by the General Data Protection Regulation (GDPR) when designing and implementing Data Protection. This guarantees that Data Protection will always be linked to true and quantified risks.

This Breach Notification Procedure offers direction to employees who have to determine the company's response to personal Data Protection breaches.

3 GENERAL DATA PROTECTION REGULATION (GDPR)

All Lothian Buses data privacy policies must be read in conjunction with 'Computer Usage and Information Security Policy'. To summarise, the key principles of the GDPR which relate to data storage and retention are:

1) Personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes, ('purpose limitation');
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, ('data minimisation');
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, ('storage limitation');
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, ('integrity and confidentiality').

4 SCOPE

The policy applies to Lothian Buses who will demonstrate accountability through compliance of the principles. This means that Lothian Buses will define measure, gather evidence and audit the business to ensure personal data is being handled lawfully.

This policy applies to:

- The senior executives of the company
- All staff within the business
- All contractors, suppliers and other people working on behalf of the business.

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR indicates that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals.

5 PERSONAL DATA DEFINITIONS

“Personal data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processing of special categories personal data” revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited, unless a lawful exemption has been identified.

A “breach” of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

“Destruction” of personal data is where the data no longer exists, or no longer exists in a form that is of any use to the controller or the Data Subject is no longer identifiable.

“Damage” is where personal data has been altered, corrupted, or is no longer complete.

“Loss” of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession.

“Unauthorised or unlawful processing” may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

6 A PERSONAL DATA PROTECTION BREACH

6.1 Scope of a Breach

The GDPR contains provisions on when a breach needs to be notified, and to whom, as well as what information should be provided as part of the notification. Information required for the

notification can be provided in phases, but in any event, controllers should act on any breach in a timely manner.

A breach can be categorised according to the following three well-known information security principles:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.

6.2 The potential detriment to data subjects:

The potential detriment to individuals is the overriding consideration in deciding whether a breach of data security should be reported to the Information Commissioners Office (ICO).

Detriment includes emotional distress as well as both physical and financial damage. Ways in which detriment can occur include:

- exposure to identity theft through the release of non-public identifiers, e.g., passport number;
- information about the private aspects of a person's life becoming known to others, e.g., financial circumstances.

The extent of detriment likely to occur is dependent on both the volume of personal data involved and the sensitivity of the data.

6.3 The volume of personal data lost / released / corrupted:

There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. It is difficult to be precise about what constitutes a large volume of personal data. Every case must be considered on its own merits.

6.4 The sensitivity of the data lost / released / corrupted:

There should be a presumption to report to the ICO where smaller amounts of personal sensitive data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.

7 REPORTING A BREACH

The Data Protection Officer of the Data Controller is responsible for reporting a breach. **The Data Protection Officer should be notified IMMEDIATELY when there has been a breach, there is a possibility of a breach occurring (near miss) or a breach has been suspected.**

7.1 Notification of a personal data breach to the ICO

If a personal data breach is judged to be a "risk" to the rights and freedoms of the data subject then Lothian Buses shall without undue delay and not later than 72 hours after having become aware of it, notify the breach to the ICO. If the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.

A third-party data processor shall notify Lothian Buses without undue delay after becoming aware of a personal data breach.

The information to be provided in the breach notification is:

a) describe the nature of the personal data breach including the categories and approximate number of data subjects concerned; and the categories and approximate number of personal data records concerned.
b) communicate the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including measures to mitigate adverse effects.

Lothian Buses will document any personal data breaches, comprising the facts relating to the breach.

7.2 Communication of a personal data breach to the data subject

When the personal data breach is likely to result in a "high risk" to the rights and freedoms of natural persons, Lothian Buses shall communicate the personal data breach to the data subject without undue delay

This communication shall:

- describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in (b), (c) and (d) of 7.1

The communication to the data subject is not required if:

(a) Lothian Buses has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the breach. e.g. an encrypted USB memory stick;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely, e.g., a mobile phone is wiped after loss;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner. e.g., a notice is published on the company website.

8 REFERENCES

Article 29 Working Party guidelines on personal data breach notification.
http://ec.europa.eu/newsroom/document.cfm?doc_id=47741

Notification of data security breaches to the ICO UK GDPR data breach reporting (DPA 2018) | ICO

Guidance on data security breach management Breach response and monitoring | ICO