Luceco Plc

Data Protection Policy

Updated 16th July 2024

Update Schedule The Data Protection Policy (the "Policy") is reviewed on an as needs basis, but no less than once in any rolling 24-month period and may be amended at any time. The Data Protection Officer ("DP Officer") will continue to review the effectiveness of this Policy to ensure it is achieving its stated objectives. Recommendations for any amendments should be emailed to the DP Officer (please refer to section 9 below for contact details).

Applicability The requirements in this Policy apply to all permanent, temporary and contract workers employed or engaged by Luceco Plc ("Luceco") (collectively hereinafter referred to as an "employee") and to any 3rd party organisations while working or engaged on Luceco business.

Compliance Any employee found to have violated this Policy could be subject to disciplinary action, up to and including termination of their employment. At its sole discretion, Luceco may require the removal from the service provision account of any employee of a 3rd party organisation contractually engaged on Luceco business, who has been evidenced to have violated this, Policy.

1. Overview

1.1 Introduction

1.1.1 Luceco Plc ("LUCECO", "we", "us" and "our") is a public limited company in the United Kingdom ("UK").

1.1.2 The UK General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018 (together referred to as "Data Protection Legislation") regulate the processing of personal data and protect the rights of the data subject.

1.1.3 As Luceco process personal data we are registered as a data controller (Registration Number ZA667736) with the Information Commissioner's Office ("ICO"), which means we are responsible for deciding how we hold and use personal data. In certain circumstances, we may be a joint data controller (please refer to section 2.5 Purposes of Processing, which refers to Luceco's Privacy Notices for more detail).

1.1.4 Data Protection Legislation imposes restrictions on how we obtain, handle, store, destroy and process personal data.

1.2 Scope

1.2.1 This Policy applies to all data subjects in relation to whom Luceco holds or has received personal data in order to carry out Luceco functions.

1.3 Risk Appetite Alignment

1.3.1 The requirements outlined within this Policy support mitigation of the following risk categories:

Level 1 Risk Category:

- Security

Level 2 Risk Category:

- Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with UK GDPR requirements.
- Compromise or loss of data confidentiality: risk of Luceco data (including GDPR relevant and Luceco sensitive data) being compromised or lost through a security incident.
- Retention or disposal: risk of Luceco data or information being compromised due to it being available or unavailable resulting in a retention or disposal issue.
- Unauthorised changes to data or systems: risk of Luceco data or systems integrity being changed/amended due to malicious activity.
- Unavailability of data or systems due to security incident: risk of Luceco data/systems being made unavailable.
- Unauthorised Access: risk of an unauthorised user (internal or external) gaining access to Luceco systems and/or data.
- Physical Security: risk of loss, theft or damage to Luceco assets or data, or adverse impacts on colleague safety as a result of inadequate physical security.
- Supplier Compromise/Breach: risk that a supplier is targeted in a cyber-attack, data theft or other security incident, impacting Luceco services and/or data.

1.3.2 Compliance with Policy requirements ensures that Luceco continues to operate within its Risk Appetite, which is overall Cautious, reflecting a preference for safe delivery options

that have a low degree of residual risk. This is principally because of the operational imperatives and secondly due to political/regulatory imperatives.

1.3.3 A number of scenarios are defined in the Information Risk Appetite Statement, where a more granular risk tolerance applies, representing a greater or lesser appetite for information risks posed by a specific system, process or asset.

1.4 Status of Policy

1.4.1 This Policy sets out Luceco's rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, and destruction of personal data.

1.4.2 Luceco's designated Data Protection Officer (DPO) is responsible for monitoring compliance with Data Protection Legislation and this Policy. Any questions or concerns about the operation of this Policy should be referred in the first instance to the DP Officer (please refer to section 9 below for contact details).

1.4.3 If you consider this Policy has not been followed, then you should raise the matter with your line manager (for Luceco employees) and/or the DP Officer.

2. Data Protection Legislation

2.1 Background

2.1.1 Data Protection Legislation regulates the processing of personal data in order to protect the interests of the data subject.

2.1.2 This covers many data protection issues in detail and therefore you may find that guidance covering some aspects of data protection are set out in more detail in separate Luceco policies and guidelines referred to within this Policy.

2.2 Definitions

2.2.1 There are a number of key definitions used within Data Protection Legislation that are essential to understanding this Policy and LUCECO's obligations under Data Protection Legislation.

"UK GDPR" means the retained EU law version of the General Data Protection Regulation (Regulation (EU) 2016/679) by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419)

"data" – means information held in an electronic form (eg. computers, personal organisers, laptops) or information held manually or in paper form as part of a filing system.

A " filing system" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

"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.

Examples of personal data include name, telephone number, age, qualifications and employment history.

“data controller” – means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
“data processor” – means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

“data protection officer” - the individual whose primary role is to ensure that their organisation processes the personal data of its employees, customers, providers or any other data subjects in compliance with the applicable Data Protection Legislation.

“data subject” – means an identified or identifiable natural person. Data subjects may include employees, contractors, customers, job applicants, candidates and suppliers; and the data processed may relate to present, past and prospective data subjects.

“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. Process and processed will be construed accordingly.

“special category data” – means 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.

2.3 Data Protection Principles
2.3.1 Luceco has a duty to ensure that all personal data (however collected) is processed in accordance with the below data protection principles, as detailed in Data Protection Legislation.

Personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
- accurate and, where necessary, be kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay (‘accuracy’);
- 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’); and
- 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, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2.4 Special Category, Criminal Convictions Data and Luceco Sensitive Information
2.4.1 Luceco employees may in certain circumstances become privy to special category and criminal convictions data.

2.4.2 Data Protection Legislation states that special category data should only be collected, processed, or disclosed in very specific circumstances eg. explicit consent, as it is recognised that the processing of this data may create significant risks to the data subject's rights and freedoms.

2.4.3 Criminal record data is not special category data, it does however have protections under Data Protection Legislation.

2.4.4 Luceco Sensitive Information - Luceco may also store and process sensitive information, not meeting the definition of special category data, but it is deemed sensitive and therefore requires additional handling arrangements. For example, bank and financial details and interview transcripts.

2.5 Purposes of Processing
2.5.1 Please see the applicable Privacy Notice for information in relation to the purpose for which personal data is processed.

- Customer Privacy policy
- Employee and applicant privacy policy

2.6 Data Retention
2.6.1 Please refer to Luceco's records management policy for more detail in relation to the period for which personal data is retained.

2.7 Rights of the Data Subject
2.7.1 Data Protection Legislation establishes rights for data subjects with regard to the processing of their personal data i.e., their right to:

- be informed about the collection and use of their personal data;
- obtain access to their personal data (please refer to section 5 for more detail);
- request to have certain personal data corrected, or completed if it is incomplete;
- have personal data erased;
- request certain personal data is restricted from processing. This enables the data subject to ask us to suspend the processing of personal data about the data subject, where for example the data subject wants us to establish its accuracy or the reason for processing;
- data portability, allowing individuals to obtain and reuse their personal data for their own purposes across different services;
- object to the processing of their personal data;
- be informed about any automated decision-making activity (including profiling);
- complain to the appropriate supervisory body eg. the Information Commissioners Office; and
- withdraw consent to personal data being processed (where consent is being relied upon by Luceco).

2.7.2 The available rights and the way to exercise them are:

- Request access to your personal information: You have a right to have access to the personal information which we hold about you, subject to certain limitations. This is referred to as a data subject access request, or DSAR. Contact the data protection officer if you wish to exercise this right.

- Request correction of your personal information: You have a right to have your personal information corrected, or rectified, if it is inaccurate or incomplete. If you become aware that any of the data which we hold about you is inaccurate, you should contact us as soon as practicable. You must notify us immediately on becoming aware of any change of circumstances which require changes to be made to any of the personal information which we hold about you.

- Request erasure (or deletion) of your personal information: You have a right to request the deletion or removal of your personal information where there is no compelling reason for its continued processing. Your right to make such a request will arise in specific circumstances, for example, where data is no longer necessary for the purpose for which it was collected or where you withdraw your consent for processing your data (and this is the sole basis on which your data is processed). If you would like to exercise this right, you must submit a written request specifying the information which you wish deleted. We will then consider this request in accordance with our obligations under data protection laws.

- Request the restriction of processing of your personal information: You have a right to block or suppress the processing of your personal information in certain circumstances. If for example you contest the accuracy of the personal data, processing may be restricted until the accuracy of the personal information has been verified. This may also apply where you contest that the processing is unlawful. If you would like to exercise this right, you must submit a written request specifying the information which you would like us to impose a processing restriction.

- Request the transfer of your personal information to another party: You have a right to obtain and re-use your personal information for your own purposes across different services – this is referred to as the right to data portability. This allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way. If you would like to exercise this right, you must submit a written request to specifying the information which you wish to be transferred. Where the right applies, we are obliged to comply with any such request within one month.

- Object to us processing your personal information: You have the right to object to the processing of your personal data if it is based on the performance of a task carried out in the public interest. If you would like to exercise this right, you must submit a written request to outlining the grounds upon which you object. We will consider any request in accordance with our obligations under data protection laws.

If you want to exercise any of these rights, please write to:
Data Protection Officer
Luceco Plc
Luceco National Distribution Centre
Stafford Park 1
Telford
TF3 3BD
Email: data.protection@luceco.com

3. Changes to Personal Data

3.1 Accuracy of Personal Data

3.1.1 Luceco is required to maintain accurate records of the personal data it processes. The accuracy of personal data is checked on regular intervals and it is of your interest to keep your personal data up to date eg. moving address.

3.2 Changes to Personal Data

3.2.1 To assist Luceco with its obligation to maintain accurate records, if a data subject's personal data changes, then this can be updated through one of the following channels:

- a customer can confirm/update their personal data by contacting our customer services team or their account manager.
- an employee can update their personal data by contacting the people team.
- a contractor should contact the People department, their business contact within Luceco or their agency;
- a supplier should contact their relevant business contact within Luceco; and data subjects who do not fall within one of the aforementioned categories, should contact the data protection office.

4. Data Sharing

4.1 Sharing and Transferring of Personal Data

4.1.1 We may need to share personal data with some third parties, including our service providers. When this occurs, Luceco require third parties to respect the security of that data and to treat it in accordance with Data Protection Legislation.

4.1.2 Luceco will only transfer personal data outside of the European Economic Area ("EEA") in limited circumstances. When this occurs, Luceco will ensure that adequate technical and organisational safeguards are in place, so that any personal data transferred remains secure and is protected.

4.1.3 For Internal Use Only: If your role within Luceco requires you to transfer data outside of the EEA, then please discuss this with the DP Officer prior to initiating any such transfer.

5. Data Subject Access Requests ("DSARs")

5.1 Contact Points for DSARs

5.1.1 Individuals that Luceco holds personal data about have the right to request a copy of their data, by phone, online e.g. social media or in writing.

5.1.2 Customers or individuals who are not Luceco employees can submit a request using the Customer or Sponsor DSAR form, and send to the address or email below:

Data Protection Officer
Luceco Plc
Luceco National Distribution Centre
Stafford Park 1
Telford
TF3 3BD
Email: data.protection@luceco.com

5.1.3 Employees/Former Employees can submit a request using the subject access request form on the Luceco Intranet and sending it to data.protection@luceco.com

5.1.4 For Internal Use Only: DSARs made to Luceco should be notified immediately to data.protection@luceco.com as a statutory time limit of one month for responding applies.

6. Security Breaches

6.1 Notification of Security Breaches

6.1.1 A security breach (which may also be referred to as a personal data breach) is considered to be 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.

6.1.2 If you become aware of a security breach or believe an event may constitute a security breach, you should raise this matter immediately:

- for internal notifications by employees, follow the internal Luceco breach management process
- for external notifications by customers, contact the company data protection officer at data.protection@luceco.com

7. Enforcement

7.1 ICO enforcement and Escalation

7.1.1 The ICO has certain enforcement powers provided under Data Protection Legislation, and may serve information, reprimands, enforcement or monetary penalty notices on an organisation, where it considers Data Protection Legislation has been breached.

7.1.2 Data Subjects have the right to make a complaint to the ICO in relation to Luceco's processing of personal data, by writing to:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF
Emailing: icocasework@ico.org.uk; or
Calling: 0303 1231113

7.1.3 For Internal Use Only: In the event that you receive a notice, or any other correspondence from the ICO, you must refer this to the DP Office immediately.

8. For Internal Use Only: Offences

8.1 Failure to comply

8.1.1 While it is Luceco's responsibility to comply with Data Protection Legislation, any failure by an employee, agent or contractor acting on behalf of Luceco to comply with this policy (or any other relevant Luceco policies, procedures or guidelines), may be constituted as a disciplinary offence.

8.1.2 Some activities may be considered gross misconduct eg.

- attempting to gain unauthorised access to restricted customer accounts as set out in the Accessing Restricted Customer Accounts Policy;
- unauthorised or unlawful obtaining, copying or disclosure of personal data under the control of Luceco;
- unauthorised selling or offering to sell personal data under the control of Luceco; and
- use of personal, or special category data, contrary to the purposes notified by Luceco.

9. Contact Details

For further guidance on this Policy please contact Luceco's DP Officer at:
Data Protection Officer
Luceco Plc
Luceco National Distribution Centre
Stafford Park 1
Telford
TF3 3BD
or email: data.protection@luceco.com