LEE-DICKENS LTD

Personal Data Protection Policy

Certificate Number FM29298

Rushton Road, Desborough, Kettering, Northants, NN14 2QW

t: +44 (0) 1536 760156 f: +44 (0) 1536 762552 e: sales@lee-dickens.co.uk

Introduction

Lee-Dickens Ltd is committed to respect the privacy of our customers, suppliers and employees and to protect their personal data accordingly.

Lee-Dickens Ltd respects the rights of all data subjects including rights of access to their data, the right of restriction of processing or erasure, and the right of accuracy. Lee-Dickens Ltd will provide clear and unambiguous information about how and why subjects' data may be collected and processed.

Contents

1 APPLICABILITY OF THIS POLICY

This policy applies to Lee-Dickens Ltd, its employees and Third Parties.

This Policy sets out the basic principles of Lee-Dickens Ltd.'s data protection and data security standards and ensures compliance the General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA).

Personal Data is any information which relates to an identified or Identifiable Natural Person. All Personal Data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process Personal Data.

An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. Lee-Dickens, as a Data Controller, is responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may expose Lee-Dickens to complaints, regulatory action, fines and/or reputational damage.

Lee-Dickens' leadership is fully committed to ensuring continued and effective implementation of this policy, and expects all Lee-Dickens' Employees and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary or legal action.

2 SCOPE

This policy applies to all aspects of Lee-Dickens' business where a Data Subject's Personal Data is stored or processed:

- In the management and administration of employees.
- In the recruitment process.
- In the context of the business activities of Lee-Dickens.
- For the provision or offer of goods or services to individuals (including those provided or offered free-of-charge) by Lee-Dickens.
- To actively monitor the behaviour of individuals, which includes using data processing techniques such as persistent web browser cookies or dynamic IP address tracking, to profile an individual with a view to:
    - Taking a decision about them.
    - Analysing or predicting their personal preferences, behaviours and attitudes.

This policy applies to all Storing and Processing of Personal Data in electronic form (including electronic mail, documents created with word processing software, and biometric data) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

3 POLICY

3.1 ACCOUNTABILITY

There shall be accountability in all processing activities. At Lee-Dickens the Managing Director is responsible for the implementation and observance of this policy and will:

- Act as a point of contact for and cooperating with Data Protection Authorities (DPAs);
- Provide guidance with regards to carrying out Data Protection Impact Assessments (DPIAs);
- Determine the need for notifications to one or more DPAs as a result of Lee-Dickens' current or intended Personal Data processing activities;
- Make and keep current notifications to one or more DPAs as a result of Lee-Dickens' current or intended Personal Data processing activities;
- Maintain a system providing prompt and appropriate responses to Data Subject requests;

3.2 DATA PROTECTION

Lee-Dickens Ltd will implement appropriate technical and organisational measures for ensuring that, by default, only personal data that is necessary for each specific purpose of the processing is processed.

The Company must ensure that a Data Protection Impact Assessment (DPIA) is conducted for all new and/or revised systems or processes for which it has responsibility. The subsequent findings of the DPIA must then be submitted to the Managing Director for review and approval.

3.3 COMPLIANCE MONITORING

To confirm that an adequate level of compliance to this policy is being achieved, the Managing Director will organise for periodic Data Protection compliance audit. Each audit will, as a minimum, assess:

- The assignment of responsibilities.
- Raising awareness.
- Training of Employees.
- The effectiveness of Data Protection related operational practices, including:
    - Data Subject rights.
    - Personal Data transfers.
    - Personal Data incident management.
    - Personal Data complaints handling.
    - The level of understanding of Data Protection policies and Privacy Notices.
    - The currency of Data Protection policies and Privacy Notices.
    - The accuracy of Personal Data being stored.
    - The conformity of Data Processor activities.
    - The adequacy of procedures for redressing poor compliance and Personal Data Breaches.

The Managing Director, in cooperation with the senior management team will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame.

3.4 DATA PROTECTION PRINCIPLES

3.4.1 Principles for processing of personal data Lawfulness, fairness and transparency.

Personal data will be collected and processed in a lawful, fair and transparent manner to protect the individual rights of the data subjects.

This means, Lee-Dickens must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

3.4.2 Restriction to a specific purpose

Personal data will only be collected for specified explicit and legitimate purposes and will not be processed in a manner incompatible with those purposes.

This means Lee-Dickens must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

3.4.3 Data economy/Data minimization

Personal data will be adequate, relevant and limited to what is necessary. Personal data will not be stored longer than necessary.

This means Lee-Dickens must not store any Personal Data beyond what is strictly required.

3.4.4 Data accuracy

Personal data will be accurate and where necessary kept up to date. Lee-Dickens Ltd will take every reasonable step to erase or rectify inaccuracies without delay.

This means Lee-Dickens must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

3.4.5 Data retention

Time limits for storage of personal data will be defined. Lee-Dickens Ltd erases personal data that is no longer necessary in relation to the purposes for which it has been collected or in a case a given consent is withdrawn and no other legitimate purpose for processing applies.

3.4.6 Security of processing/Data security

Personal data will be processed securely. Appropriate to the risk, technical and organisational measures will be taken against unauthorised processing or alteration, and against loss or destruction or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. Lee-Dickens Ltd will ensure ongoing integrity, availability, confidentiality and authenticity.

Lee-Dickens Ltd will ensure resilience of our systems and services processing personal data. In the event of an incident Lee-Dickens Ltd will have the ability to restore the availability and access to data in a timely manner.

3.5 DATA COLLECTION

3.5.1 Data Sources

Personal Data should be collected only from the Data Subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the Personal Data from other

persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the Data Subject or to prevent serious loss or injury to another person.

If Personal Data is collected from someone other than the Data Subject, the Data Subject must be informed[1] of the collection unless one of the following apply:
- The Data Subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, Processing or transfer of the Personal Data.

Where it has been determined that notification to a Data Subject is required notification should occur promptly, but in no case later than:
- One calendar month from the first collection or recording of the Personal Data.
- At the time of first communication if used for communication with the Data Subject.
- At the time of disclosure if disclosed to another recipient.

3.5.2 Data Subject Consent

Lee-Dickens will obtain Personal Data only by lawful and fair means and, where appropriate with the knowledge and Consent of the individual concerned. Where a need exists to request and receive the Consent of an individual prior to the collection, use or disclosure of their Personal Data, Lee-Dickens is committed to seeking such Consent.

The management team shall establish a system for obtaining and documenting Data Subject Consent for the collection, Processing, and/or transfer of their Personal Data. The system must include provisions for:
- Determining what disclosures should be made in order to obtain valid Consent.
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the Consent is freely given (i.e. is not based on a contract that is conditional to the Processing of Personal Data that is unnecessary for the performance of that contract).
- Documenting the date, method and content of the disclosures made, as well as the validity, scope, and volition of the Consents given.
- Providing a simple method for a Data Subject to withdraw their Consent at any time.

3.5.3 Data Subject Notification

Lee-Dickens will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide Data Subjects with information as to the purpose of the Processing of their Personal Data. When the Data Subject is asked to give Consent to the Processing of Personal Data and when any Personal Data is collected from the Data Subject, all appropriate disclosures[2] will be made, in a manner that draws attention to them, unless one of the following apply:
- The Data Subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent.

1 A list of the disclosures that need to be made available to the Data Subject is provided in section 5.2 - APPENDIX 2 - Information Notification to Data Subjects.
2 A list of the disclosures that need to be made available to the Data Subject is provided in section 5.2 - APPENDIX 2 - Information Notification to Data Subjects.

The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Managing Director. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

3.5.4 External Privacy Notices

Each external website provided by Lee-Dickens will include the Company's downloadable 'Privacy Notice for Third Parties'.

3.6 DATA USE

3.6.1 Data Processing

Lee-Dickens uses the Personal Data of its Contacts for the following broad purposes:

- In the management and administration of employees.
- In the recruitment process.
- The general running and administration of the business.
- To provide, administer and manage services for Lee-Dickens customers.

The use of a Contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a Contact's expectations that their details will be used by Lee-Dickens to respond to a Contact request for information about the products and services on offer. However, it will not be within their reasonable expectations that Lee-Dickens would then provide their details to Third Parties for marketing purposes.

Lee-Dickens will Process Personal Data in accordance with all applicable laws and applicable contractual obligations. More specifically, Lee-Dickens will not Process Personal Data unless at least one of the following requirements are met:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Company is subject.
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company.
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject).

There are some circumstances in which Personal Data may be further processed for purposes that go beyond the original purpose for which the Personal Data was collected. When making a determination as to the compatibility of the new reason for Processing, guidance and approval must be obtained from the Managing Director before any such Processing may commence.

In any circumstance where Consent has not been gained for the specific Processing in question, Lee-Dickens will address the following additional conditions to determine the fairness and transparency of any Processing beyond the original purpose for which the Personal Data was collected:

- Any link between the purpose for which the Personal Data was collected and the reasons for intended further Processing.
- The context in which the Personal Data has been collected, in particular regarding the relationship between Data Subject and the Company.
- The nature of the Personal Data, in particular whether Special Categories of Data are being Processed, or whether Personal Data related to criminal convictions and offences are being Processed.
- The possible consequences of the intended further Processing for the Data Subject.
- The existence of appropriate safeguards pertaining to further Processing, which may include Encryption, Anonymisation or Pseudonymisation.

3.6.2 Special Categories of Data

Lee-Dickens will only Process Special Categories of Data (also known as sensitive data) where the Data Subject expressly consents to such Processing or where one of the following conditions apply:

- The Processing relates to Personal Data which has already been made public by the Data Subject.
- The Processing is necessary for the establishment, exercise or defence of legal claims.
- The Processing is specifically authorised or required by law.
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent.
- Further conditions, including limitations, based upon national law related to the Processing of genetic data, biometric data or data concerning health.

In any situation where Special Categories of Data are to be Processed, prior approval must be obtained from the Managing Director and the basis for the Processing clearly recorded with the Personal Data in question. Where Special Categories of Data are being Processed, Lee-Dickens will adopt additional protection measures. Lee-Dickens may also adopt additional measures to address local custom or social expectation over the Processing of Special Categories of Data.

3.6.3 Children's Data

Children[3] are unable to Consent to the Processing of Personal Data for information society services[4]. Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where Processing is lawful under other grounds, Consent need not be obtained from the child or the holder of parental responsibility.

Should Lee-Dickens foresee a business need for obtaining parental consent for information society services offered directly to a child, guidance and approval must be obtained from the Managing Director before any Processing of a child's Personal Data may commence.

3.6.4 Data Quality

Lee-Dickens will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate in the first instance, and is updated to reflect the current situation of the Data Subject. The measures adopted by Lee-Dickens to ensure data quality include:

[3] The age by which an individual is legally designated a child varies but in the UK is currently (April 2018) 13 years.
[4] Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification.
- Keeping Personal Data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of Personal Data if in violation of any of the Data Protection principles or if the Personal Data is no longer required.
- Quarantining, rather than deletion of Personal Data, insofar as:
  - a law prohibits erasure.
  - erasure would impair legitimate interests of the Data Subject.
  - the Data Subject disputes that their Personal Data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

3.6.5 Profiling & Automated Decision-Making

Lee-Dickens will only engage in Profiling and automated decision-making where it is necessary to enter into, or to perform, a contract with the Data Subject or where it is authorised by law. Where Lee-Dickens utilises Profiling and automated decision-making, this will be disclosed to the relevant Data Subjects. In such cases the Data Subject will be given the opportunity to:

- Express their point of view.
- Obtain an explanation for the automated decision.
- Review the logic used by the automated system.
- Supplement the automated system with additional data.
- Have a human carry out a review of the automated decision.
- Contest the automated decision.
- Object to the automated decision-making being carried out.

Lee-Dickens must also ensure that all Profiling and automated decision-making relating to a Data Subject is based on accurate data.

3.6.6 Digital Marketing

As a general rule Lee-Dickens will not send promotional or direct marketing material to a Personal Data Subject through digital channels such as mobile phones, email and the Internet, without first obtaining their Consent. If the Company wish to carry out a digital marketing campaign without obtaining prior Consent from the Personal Data Subject must first have it approved by the Managing Director.

Where Personal Data Processing is approved for digital marketing purposes, the Data Subject must be informed at the point of first contact that they have the right to object, at any stage, to having their data Processed for such purposes. If the Data Subject puts forward an objection, digital marketing related Processing of their Personal Data must cease immediately and their details should be kept on a suppression list with a record of their opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain an indication of Consent to carry out digital marketing to individuals provided that they are given the opportunity to opt-out.

3.7 DATA RETENTION

To ensure fair Processing, Personal Data will not be retained by Lee-Dickens for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further Processed. The length of time for which Lee-Dickens needs to retain Personal Data will take into

account legal and contractual requirements, both minimum and maximum. All Personal Data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

3.8 DATA PROTECTION

Lee-Dickens will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment.

Lee-Dickens will:

- Prevent unauthorised persons from gaining access to data processing systems in which Personal Data are Processed.
- Prevent persons entitled to use a data processing system from accessing Personal Data beyond their needs and authorisations.
- Ensure that Personal Data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that access logs are in place to establish whether, and by whom, the Personal Data was entered into, modified on or removed from a data processing system.
- Ensure that in the case where Processing is carried out by a Data Processor, the data can be Processed only in accordance with the instructions of the Company.
- Ensure that Personal Data is protected against undesired destruction or loss.
- Ensure that Personal Data collected for different purposes can and is Processed separately.
- Ensure that Personal Data is not kept longer than necessary.

3.9 DATA SUBJECT REQUESTS

The Company will establish a system to enable and facilitate the exercise of Data Subject rights related to:

- Information access.
- Objection to Processing.
- Objection to automated decision-making and profiling.
- Restriction of Processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, Lee-Dickens will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature.

Data Subjects are entitled to obtain, based upon a request made in writing to the Managing Director and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, Processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the

storage period.
- The use of any automated decision-making, including Profiling.
- The right of the Data subject to:
  - object to Processing of their Personal Data.
  - lodge a complaint with the Data Protection Authority.
  - request rectification or erasure of their Personal Data.
  - request restriction of Processing of their Personal Data.

All requests received for access to or rectification of Personal Data must be directed to the Managing Director, who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require Lee-Dickens to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If Lee-Dickens cannot respond fully to the request within 30 days, the Managing Director shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:
- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- An estimate of any costs to be paid by the Data Subject (e.g. where the request is excessive in nature).
- The name and contact information of the Lee-Dickens individual who the Data Subject should contact for follow up.

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

3.10 LAW ENFORCEMENT REQUESTS & DISCLOSURES

In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:
- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If Lee-Dickens Processes Personal Data for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question.

If Lee-Dickens receives a request from a court or any regulatory or law enforcement authority for information relating to a Lee-Dickens Contact, you must immediately notify the Managing Director who will provide comprehensive guidance and assistance.

3.11 DATA PROTECTION TRAINING

All Lee-Dickens Employees that have access to Personal Data will have their responsibilities under this policy outlined to them as part of their staff training. In addition, Lee-Dickens will provide regular Data Protection training and procedural guidance for their staff.

The training and procedural guidance will consist of, at a minimum, the following elements:

- The Data Protection Principles set forth in Section 3.4 above.
- Each Employee's duty to use and permit the use of Personal Data only by authorised persons and for authorised purposes.
- The need for, and proper use of, the forms and procedures adopted to implement this policy.
- The correct use of passwords, security tokens and other access mechanisms.
- The importance of limiting access to Personal Data, such as by using password protected screen savers and logging out when systems are not being attended by an authorised person.
- Securely storing manual files, print outs and electronic storage media.
- The need to obtain appropriate authorisation and utilise appropriate safeguards for all transfers of Personal Data outside of the internal network and physical office premises.
- Proper disposal of Personal Data by using secure shredding facilities.
- Any special risks associated with particular departmental activities or duties.

3.12 DATA TRANSFERS

Lee-Dickens may transfer Personal Data to internal or Third Party recipients located in another country where that country is recognised as having an adequate level of legal protection[5] for the rights and freedoms of the relevant Data Subjects.

Where transfers need to be made to countries lacking an adequate level of legal protection (i.e. Third Countries), they must be made in compliance with an approved transfer mechanism[6].

Lee-Dickens may only transfer Personal Data where one of the transfer scenarios list below applies:

- The Data Subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the Data Subject.
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the Data Subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a Third Party in the interest of the Data Subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the Data Subject.

3.12.1 Transfers to Third Parties

Lee-Dickens will only transfer Personal Data to, or allow access by, Third Parties when it is assured that the information will be Processed legitimately and protected appropriately by the recipient. Where

[5] For an up to date list of countries recognised as having an adequate level of legal protection, refer to the Information Commissioner's Office website: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/

[6] For an up to date list of Third Country transfer mechanisms recognised as providing adequate protection, refer to the ICO website: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-8-international/

Third Party Processing takes place, Lee-Dickens will first identify if, under applicable law, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, Lee-Dickens will enter into an appropriate agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data transferred.

Where the Third Party is deemed to be a Data Processor, Lee-Dickens will enter into a Processing agreement with the Data Processor. The agreement must require the Data Processor to protect the Personal Data from further disclosure and to only Process Personal Data in compliance with Lee-Dickens instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

When Lee-Dickens is outsourcing services to a Third Party (including Cloud Computing services), they will identify whether the Third Party will Process Personal Data on its behalf and whether the outsourcing will entail any Third Country transfers of Personal Data. In either case, it will make sure to include adequate provisions in the outsourcing agreement for such Processing and Third Country transfers.

The Managing Director shall conduct regular audits of Processing of Personal Data performed by Third Parties, especially in respect of technical and organisational measures they have in place. Any major deficiencies identified will be reported to and monitored by the Lee-Dickens Management team.

3.13 COMPLAINTS HANDLING

Data Subjects with a complaint about the Processing of their Personal Data, should put forward the matter in writing to the Managing Director. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Managing Director will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and the Managing Director, then the Data Subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

3.14 BREACH REPORTING

Any individual who suspects that a Personal Data Breach has occurred due to the theft or exposure of Personal Data must immediately notify the Managing Director providing a description of what occurred. Notification of the incident can me made via e-mail data-protection@lee-dickens.co.uk, by calling +44 1536 760156, or by letter addressed to the Managing Director.

The Managing Director will investigate all reported incidents to confirm whether or not a Personal Data Breach has occurred. If a Personal Data Breach is confirmed, the Managing Director will follow the relevant authorised procedure based on the criticality and quantity of the Personal Data involved. For severe Personal Data Breaches, the Managing Director will initiate and chair an emergency response team to coordinate and manage the Personal Data Breach response.

GDPR requires that as soon as the Controller becomes aware that a personal data breach has occurred, the Controller should notify the personal data breach to the ICO without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the Controller is able to

demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

4 POLICY REVIEW

This policy will be reviewed periodically, ensuring the alignment of this policy with Data Protection regulations, national law or Union based Data Protection provisions.

5 APPENDICES

5.1 APPENDIX 1 - DEFINITIONS

Anonymisation - Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) by any means or by any person.

Binding Corporate Rules - The Personal Data protection policies used for the transfer of Personal Data to one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Company - Lee-Dickens Ltd. Registered in England No. 735448. VAT Number GB120027046. D-U-N-S 218621498. Quality Management System Registration No. FM29298

Consent - Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Contact - Any past, current or prospective Lee-Dickens customer.

Data Controller - A 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 Processors - A natural or legal person, Public Authority, Agency or other body which Processes Personal Data on behalf of a Data Controller.

Data Protection - The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.

Data Protection Authority - An independent Public Authority responsible for monitoring the application of the relevant Data Protection regulation set forth in national law. In the UK it is the ICO.

Data Subject - The identified or Identifiable Natural Person to which the data refers.

Employee - An individual who works part-time or full-time for Lee-Dickens under a contract of employment, whether oral or written, express or implied, and has recognised rights and duties. Includes temporary employees and independent contractors.

Encryption - The process of converting information or data into code, to prevent unauthorised access.

Identifiable Natural Person - Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Information Commissioner's Office (ICO) - The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Personal Data - Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person.

Personal Data Breach - 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.

Process, Processed, Processing - Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include 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.

Profiling - Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

Pseudonymisation - Data amended in such a way that no individuals can be identified from the data (whether directly or indirectly) without a "key" that allows the data to be re-identified.

Special Categories of Data - Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Third Country - Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

Third Party - An external organisation with which Lee-Dickens conducts business and is also authorised by Lee-Dickens to Process the Personal Data of Lee-Dickens Contacts.

5.2 APPENDIX 2 - INFORMATION NOTIFICATION TO DATA SUBJECTS

The table below outlines the various information elements that must be provided by the Data Controller to the Data Subject depending upon whether or not Consent has not been obtained from the Data Subject.

Information Requiring Notification	With Consent	Without Consent
The identity and the contact details of the Data Controller and, where applicable, of the Data Controller's representative.	✓	✓
The original source of the Personal Data, and if applicable, whether it came from a publicly accessible source.	***X***	✓
The contact details of the Data Protection Officer, where applicable.	✓	✓
The purpose(s) and legal basis for Processing the Personal Data.	✓	✓
The categories of Personal Data concerned.	✓	✓
The recipients or categories of recipients of the Personal Data.	✓	✓
Where the Data Controller intends to further Process the Personal Data for a purpose other than that for which the Personal Data was originally collected, the Data Controller shall provide the Data Subject, prior to that further Processing, with information on that other purpose.	✓	✓
Where the Data Controller intends to transfer Personal Data to a recipient in a Third Country, notification of that intention and details regarding adequacy decisions taken in relation to the Third Country must be provided.	✓	✓
The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.	✓	✓
Where applicable, the legitimate interests pursued by the Data Controller or by a Third Party.	✓	✓
The existence of Data Subject rights allowing them to request from the Data Controller- information access, objection to Processing, objection to automated decision-making and profiling, restriction of Processing, data portability, data rectification and data erasure.	✓	✓
Where Processing is based on Consent, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal.	✓	***X***
The right to lodge a complaint with a Data Protection Authority.	✓	✓
The existence of automated decision-making (including Profiling) along with meaningful information about the logic involved and the significance of any envisaged consequences of such Processing for the Data Subject.	✓	✓
Whether the provision of Personal Data is a statutory or contractual requirement, a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and if so the possible consequences of failure to provide such data.	✓	✓