



Data Protection Policy



Quick Summary

The European Union General Data Protection Regulation (EU GDPR), the UK General Data Protection Regulation (UK GDPR 2021) and the Data Protection Act 2018 (DPA 2018) and the **Data (Use and Access) Act (DUAA 2025)** constitute the regulatory framework for data protection in the United Kingdom and European Union. This framework introduces a set of obligations imposed on organisations in relation to data protection, that Sue Lilly and Green Man Essences must comply with. This policy is designed to set out the standards that Sue Lilly and Green Man Essences must adhere to when processing personal data.

Contents

Data Protection Policy	1
Quick Summary	1
Contents	2
1. Who is covered by this policy	3
2. Why do we need this policy	3
3. What information is in scope	3
4. What counts as 'processing'	3
5. The Principles	3
6. The lawful grounds for processing data	4
7. Protection of individual rights	4
8. Retention of personal data	4
9. Data breaches	4
10. Records of personal data	4
11. Risk assessments	5
12. International personal data transfers	5
13. Security, integrity and confidentiality	5
14. Training and supervision	6
15. Our commitment	6
16. Your obligations	6
17. Why do you need to comply with this policy?	7
18. Definitions	8
Appendix 1 - The data protection principles	11
Appendix 2 - The legal grounds for processing	13
Appendix 3 - The rights available to individuals	14

1. Who is covered by this policy

This policy extends to everyone who comes across and processes personal data at Sue Lilly and Green Man Essences, including employees, contractors, temporary staff, partner organisations and any other party utilising Sue Lilly and Green Man Essences information resources. Any questions regarding this policy or any other aspect of data protection compliance should be referred to the Primary Security Contact.

2. Why do we need this policy

The regulatory framework for data protection covers the collection, storage, processing and distribution of personal data. It gives rights to individuals about whom information is recorded (data subjects) and provides a set of principles that organisations must comply with when processing personal data. The purpose of this policy is to provide guidance to members of staff at Sue Lilly and Green Man Essences on our standards and the procedures to be followed in order to achieve compliance with the requirements of the regulatory framework. This policy is intended for internal use.

3. What information is in scope

All personal data, including special categories of personal data and criminal offence data, held by Sue Lilly and Green Man Essences is in scope of the regulatory framework.

This includes, among other things, names, email addresses, phone numbers, bank details, images of the individual, opinions about that individual stated by others, expressions, actual or intended actions which relate to that individual, conversations to/from and about that individual, interview notes, credit check results, HR records, background checks, KYC checks, etc.

4. What counts as 'processing'

The term "processing" is very broad. It essentially means anything that is done to, or with, personal data (including simply collecting, storing or deleting that data); it is essentially anything done by an organisation that involves or affects personal data.

5. The Principles

Data protection principles lie at the heart of most regulatory frameworks for data protection, including the UK and EU GDPR. They are set out right at the start of the legislation, and inform everything that follows. They don't give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions.

Compliance with the spirit of these key principles is a fundamental building block for good data protection practice that Sue Lilly and Green Man Essences aims to achieve.

The principles are available in [Appendix 1](#) and are being referred to throughout this policy.

6. The lawful grounds for processing data

There are various lawful grounds for processing personal data that are available and can be used by Sue Lilly and Green Man Essences and these are available in [Appendix 2](#).

In order to collect and process personal data for any specific purpose, Sue Lilly and Green Man Essences must always have a lawful basis for doing so. Without a lawful basis for processing, the use of personal data will be unlawful and may have an adverse impact on the affected data subjects. No data subject should be surprised to learn that their personal data has been collected, consulted, used or otherwise processed by Sue Lilly and Green Man Essences .

7. Protection of individual rights

The regulatory framework provides data subjects with a number of rights in relation to their personal data. These are included in [Appendix 3](#). Sue Lilly and Green Man Essences aims to safeguard these rights and have procedures internally for any rights requests to be actioned in time and in a compliant manner.

Our approach to handling individual rights requests is documented in the Information Rights Requests Policy.

8. Retention of personal data

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes and must be securely deleted when it has achieved its purpose for processing. Sue Lilly and Green Man Essences has established procedures for determining the data retention requirements applicable and removing personal data from Sue Lilly and Green Man Essences systems once its retention period has expired. These are all documented in our Retention Policy, supplemented by the Retention Schedule.

9. Data breaches

In certain circumstances, the legal framework will require Sue Lilly and Green Man Essences to notify the Information Commissioner (IC), and potentially data subjects, of any personal data breaches that pose a high risk to individual's rights and freedoms.

Sue Lilly and Green Man Essences has put in place appropriate procedures to deal with any personal data breach and will notify the IC and/or data subjects where Sue Lilly and Green Man Essences is legally required to do so.

10. Records of personal data

Sue Lilly and Green Man Essences must keep full and accurate records of all its processing activities, in accordance with the UK and EU GDPR's requirements. Sue Lilly and Green Man Essences has put together a Record of Processing Activities (ROPA) that is reviewed and updated as and when new types of processing take place.

11. Risk assessments

A Data Protection Impact Assessment (DPIA), also known as a Privacy Impact Assessment, is a process to help identify and minimise the data protection risks involved in projects, processes and activities involving the processing of personal data. DPIAs are required for processing likely to result in high risk to the individuals and their personal data, and where new technologies are involved. In practice, Sue Lilly and Green Man Essences requires a DPIA for any projects involving the use of personal data, including new systems, solutions or projects.

DPIAs need to be assessed by the Data Protection Officer – Mrs S E Lilly

12. International personal data transfers

The EU and UK GDPR prohibit the transfer of personal data outside of the EEA in most circumstances in order to ensure that personal data is not transferred to a country that does not provide the same level of protection for the rights of data subjects. In this context, a “transfer” of personal data includes transmitting, sending, viewing or accessing personal data in or to a different country.

Sue Lilly and Green Man Essences may only transfer personal data outside of the EEA if one of the following conditions applies:

- personal data is transferred to a country deemed adequate by the EU Commission and the UK. A current list of these countries is available [here](#).
- appropriate safeguards have been implemented following a transfer risk assessment, such as:
 - Standard Contractual Clauses (SCCs) that have been approved by the European Commission and complemented by the UK Addendum to the EU SCCs, or
 - the UK’s International Data Transfer Agreement (IDTA).
- the data subject has given their explicit consent to the proposed transfer, having been fully informed of any potential risks.
- the transfer is necessary in order to perform a contract between Sue Lilly and Green Man Essences and a data subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the data subject in circumstances where the data subject is incapable of giving consent or it is a one-off restricted transfer and it is in the company’s compelling legitimate interests that the transfer is completed.

13. Security, integrity and confidentiality

The personal data that Sue Lilly and Green Man Essences collects and processes must be secured by appropriate technical and organisational measures against accidental loss, destruction or damage, and against unauthorised or unlawful processing.

Sue Lilly and Green Man Essences will develop, implement and maintain appropriate technical and organisational measures for the processing of personal data taking into account the:

- nature, scope, context and purposes for such processing
- volume of personal data processed
- likelihood and severity of the risks of such processing for the rights of data subjects.

Sue Lilly and Green Man Essences will regularly evaluate and test the effectiveness of such measures to ensure that they are adequate and effective.

14. Training and supervision

Sue Lilly and Green Man Essences will provide awareness training to all members of staff and organisations within the remit of this policy to ensure that they understand their responsibilities and the legal and other consequences that could result from non-compliance.

It is the responsibility of members of staff and line managers to ensure that training is completed in time and that members of staff are aware of their responsibilities under the data protection law.

15. Our commitment

As a data controller and data processor, Sue Lilly and Green Man Essences will:

- Ensure that all persons and organisations within the remit of this policy are made aware of their responsibilities under the data protection regulatory framework by providing them with a copy of this policy and good practice guidance.
- Provide awareness training to all persons and organisations within the remit of this policy to ensure that they understand their responsibilities, and the legal and other consequences that could result from non-compliance.
- Provide secure personal data systems, both manual and computerised, so that all those dealing with such data within Sue Lilly and Green Man Essences are able to take appropriate security measures.
- Ensure that all Sue Lilly and Green Man Essences personal data recipient organisations (e.g. suppliers and other third parties) are made aware of this policy, and related policies.
- Ensure suitable arrangements are in place in respect of services provided in partnership with other organisations.
- Ensure that all organisations who provide services on behalf of Sue Lilly and Green Man Essences understand their responsibilities under the regulatory framework for data protection.

Appendix 1 - The data protection principles

Article 5 of the UK GDPR sets out seven key principles which lie at the heart of the general data protection regime:

Lawfulness, Fairness and Transparency

All data must be processed lawfully, fairly and in a transparent manner in relation to individuals

Purpose Limitation

All data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

Data Minimisation

All data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Accuracy

All data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

Storage Limitation

All data must be 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals

Integrity and Confidentiality

All data must be 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

Accountability

Sue Lilly and Green Man Essences shall be responsible for, and be able to demonstrate compliance with the data protection principles.

Appendix 2 - The legal grounds for processing

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these will apply whenever Sue Lilly and Green Man Essences processes personal data:

Consent

The individual has given clear consent for Sue Lilly and Green Man Essences to process their personal data for a specific purpose.

Contract

The processing is necessary for a contract Sue Lilly and Green Man Essences has with the individual, or because they have asked Sue Lilly and Green Man Essences to take specific steps before entering into a contract.

Legal Obligation

The processing is necessary for Sue Lilly and Green Man Essences to comply with the law (not including contractual obligations).

Vital Interests

The processing is necessary to protect someone's life.

Public Task

The processing is necessary for Sue Lilly and Green Man Essences to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Legitimate Interests

The processing is necessary for Sue Lilly and Green Man Essences legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Appendix 3 - The rights available to individuals

The data protection regulatory framework provides the following rights for individuals:

The right to be informed

The right to be informed covers some of the key transparency requirements of the UK and EU GDPR. It is about providing individuals with clear and concise information about what we do with their personal data. We comply with this requirement by setting out all our processing activities in our privacy notice.

The right of access

The right of access is also known as a Data Subject Access Request (DSAR). This gives individuals the right to obtain a copy of the personal data that Sue Lilly and Green Man Essences stores about them, as well as other supplementary information that clarifies the processing of that personal data. It includes opinions of individuals about the requester, interview notes, meeting notes and any other personal data stored about a particular individual.

The right to rectification

Individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed, although this will depend on the purposes for the processing. This may involve the individual providing a supplementary statement to the incomplete data or asking for their records to be updated (i.e. if they have changed their name or address, etc.).

The right to erasure

Individuals have the right to have personal data erased. The right only applies to data held at the time the request is received; it does not apply to data that may be created in the future. The right is also not absolute and only applies in certain circumstances.

It does not apply to information required for compliance with a legal obligation; this means that if Sue Lilly and Green Man Essences is required by law to process an individuals' personal data, the right to erasure will not apply. It also does not apply if the purpose of the data processed is the establishment, exercise or defence of legal claims.

The right to restrict processing

Individuals have the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way in which Sue Lilly and Green Man Essences uses their data.

This right applies where individuals have a particular reason for requesting the restriction. This may be because they have issues with the content of the information held about them or the way in which Sue Lilly and Green Man Essences processes their data. In most cases this will apply for a certain period of time and will not be indefinitely.

The right to data portability

The right to data portability gives individuals the right to receive personal data they have provided to Sue Lilly and Green Man Essences in a structured, commonly used and machine readable format. Individuals can also request that a controller transmits this data directly to another controller.

The right to object

This gives individuals the right to object to the processing of their personal data at any time. It allows individuals to stop or prevent companies from processing their personal data. An objection may be in relation to all of the personal data held about an individual or only to certain information. It may also only relate to a particular purpose the data is processed for.

Rights in relation to automated decision making and profiling

The UK and EU GDPR restrict companies from making solely automated decisions that have a legal or similarly significant effect on individuals. These types of data processing can be done only in limited circumstances if:

- the data is necessary for entering into or performance of a contract with the individual;
- authorised by law (for example, for the purposes of fraud or tax evasion); or
- based on the individual's explicit consent.