V6

We take your privacy seriously; we're sure you do too, so please do have a read of the full policy.

We realise it's quite long, so we've tried to help you out by summarising it here, but we'd still love you to take the time to read it in full. In summary:

- We collect information (including sensitive information) to make Lush's website useful to you.
- We'll keep you posted with Lush news if you opt in.
- We may share your information with companies we work with, but you won't be plagued with irrelevant material. It will not be publicly available, although we may have to pass on your details where required by law or if you breach our Content Standards.
- By giving us this data, you agree it may be stored and processed outside the European Economic Area. We do all we can to ensure this is done securely and in accordance with the privacy policy.
- To remember you, our system will store cookies. This helps us to improve the website, although you can opt out.
- We will never sell your data.

V6

CONTENTS

CLAUSE

Introduction

Welcome to the Lush Group's privacy notice.

The Lush Group respects your privacy and is committed to protecting your personal data. This privacy notice will inform you as to how we look after your personal data when you visit our website (regardless of where you visit it from) and tell you about your privacy rights and how the law protects you.

This privacy notice is provided in a layered format so you can click through to the specific areas set out below. Please also use the Glossary to understand the meaning of some of the terms used in this privacy notice.

1. Important information and who we are

Purpose of this privacy notice

This privacy notice aims to give you information on how The Lush Group collects and processes your personal data through your use of this website, including any data you may provide through this website when you sign up to our newsletter, purchase a product or service or take part in a competition or event.

This website is not intended for children and we do not knowingly collect data relating to children.

It is important that you read this privacy notice together with any other privacy notice or fair processing notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This privacy notice supplements the other notices and is not intended to override them.

Controller

Lush Limited and its subsidiaries and affiliates, are referred to as 'The Lush Group'. This privacy notice is issued on behalf of Lush Limited and its subsidiaries so when we mention "Lush", "we", "us" or "our" in this privacy notice, we are referring to the relevant company in the Lush Group responsible for processing your data. Each entity which collects or receives your data under the privacy notice does so as a data controller. Certain group entities within Lush may have specific privacy notices on their websites, so when visiting or using these services please make sure you are informed of how they also use your information.

We will let you know which entity will be the controller for your data when you purchase a product or service with us. Lush Retail Limited is the controller and responsible for this UK website.

If you have any questions about this privacy notice, including any requests to exercise *your legal rights*, please contact Customer Care using the details set out below.

..

Contact details

Our full details are:

Full name of legal entity: Lush Limited

Email address: wecare@lush.co.uk

Postal address: Lush Customer Care, Poole Quay, Unit 26b Dolphin Quays, Poole, Dorset, BH15 1HU

Telephone number: +44 (0) 1202 668545

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

Changes to the privacy notice and your duty to inform us of changes

This version was last updated on 24 May 2018.

The data protection law in the UK will change on 25 May 2018. Although this privacy notice sets out most of your rights under the new laws, we may not yet be able to respond to some of your requests (for example, a request for the transfer of your personal data) until May 2018 as we are still working towards getting our systems ready for some of these changes.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

Third-party links

This website may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy statements. When you leave our website, we encourage you to read the privacy notice of every website you visit.

2. The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

We may collect, use, store and transfer different kinds of personal data about you which we have grouped together follows:

- **Identity Data** includes first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender.
- **Contact Data** includes billing address, delivery address, email address and telephone numbers.

- **Financial Data** includes bank account and payment card details.
- **Transaction Data** includes details about payments to and from you and other details of products and services you have purchased from us.
- **Technical Data** includes internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access this website.
- **Profile Data** includes your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses.
- **Usage Data** includes information about how you use our website, products and services.
- **Marketing and Communications Data** includes your preferences in receiving marketing from us and our third parties and your communication preferences.

We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data may be derived from your personal data but is not considered personal data in law as this data does **not** directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this privacy notice.

We do not collect any **Special Categories of Personal Data** about you (this includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data). Nor do we collect any information about criminal convictions and offences.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with goods or services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

3. How is your personal data collected?

We use different methods to collect data from and about you including through:

- **Direct interactions.** You may give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:
  - apply for our products or services;
  - create an account on our website;
  - subscribe to our service or publications;
  - engage with us on social media;
  - download and install apps;

- request marketing to be sent to you;
- enter a competition, promotion or survey, attend an event; or
- give us some feedback or make a complaint.

- **Automated technologies or interactions.** As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. We may also receive Technical Data about you if you visit other websites employing our cookies. Please see our cookie policy below for further details.

4. How we use your personal data

We will only use your personal data when the law allows us to and we will never sell your data to third parties. Most commonly, we will use your personal data in the following circumstances:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where we need to comply with a legal or regulatory obligation.

Except for marketing communications, generally we do not rely on consent as a legal basis for processing your personal data.

Purposes for which we will use your personal data

We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose/Activity	**Lawful basis for processing**
To register you as a new customer	(a) Performance of a contract with you
To process and deliver your order for products or services including: (a) Manage payments, fees and charges (b) Collect money owed to us	(a) Performance of a contract with you (b) Necessary for our legitimate interests
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or privacy policy (b) Asking you to leave a review or take a survey	(a) Performance of a contract with you (b) Necessary to comply with a legal obligation (c) Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)

To enable you to partake in a prize draw, event, competition or complete a survey	(a) Performance of a contract with you (b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business)
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) (b) Necessary to comply with a legal obligation
To deliver relevant website content to you and measure or understand the effectiveness of the marketing we serve to you	(a) Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	(a) Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To make suggestions and recommendations to you about goods or services that may be of interest to you	(a) Necessary for our legitimate interests (to develop our products/services and grow our business)
To carry out email marketing and send you marketing communications by email. Such communications will include information about the products, services, events, offers and promotions we offer from time to time.	(a) Where you have expressly consented to receive such marketing communications or where we have another lawful right to do so

Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of this website may become inaccessible or not function properly. For more information about the cookies we use, please see Cookie Policy below.

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

5. Disclosures of your personal data

We sometimes share your personal data with trusted third parties when we are legally permitted to do so, for example, other organisations within our group, third-party organisations that provide applications/functionality, data processing or IT services, delivery couriers, third-party organisations that assist us with the administration of our promotions, recruitment agencies and related organisations, auditors, lawyers, accountants and other professional advisers, law enforcement or other government and regulatory agencies, credit card and payment providers, third party email marketing and CRM specialists, and other third parties to help us personalise our offers to you and to fulfil our obligations to our customers.

Such third parties include but are not limited to:

- Internal Third Parties as set out in the Glossary below.
- External Third Parties as set out in the Glossary below.
- Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your personal data in the same way as set out in this privacy notice.

When we share personal information with others, we put contractual arrangements and security mechanisms in place to protect the personal information and to comply with our data protection, confidentiality and security standards but we will never sell your data to third parties.

6. International transfers

Where necessary in order to deliver our services, we will transfer personal information to countries outside the EEA. When doing so, we will comply with our legal and regulatory obligations in relation to the personal information including having a lawful basis for transferring personal information and

putting appropriate safeguards in place to ensure an adequate level of protection for the personal information.

7. Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We secure access to all transactional areas of our websites and apps using 'https' technology.

We regularly monitor our system for possible vulnerabilities and attacks, and we carry out vulnerability testing to identify ways to further strengthen security.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

8. Data retention

How long will you use my personal data for?

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

At the end of that retention period, your data will either be deleted completely or anonymised, for example by aggregation with other data so that it can be used in a non-identifiable way for statistical analysis and business planning.

9. Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your personal data. If you wish to exercise any of the rights set out below, please contact us at *wecare@lush.co.uk* for the relevant data request form.

- **Request access** to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised

your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

- **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.
- **Request restriction of processing** of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- **Request the transfer** of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
- **Withdraw consent at any time** where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

10. Glossary

LAWFUL BASIS

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

Performance of Contract means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract.

Comply with a legal or regulatory obligation means processing your personal data where it is necessary for compliance with a legal or regulatory obligation that we are subject to.

THIRD PARTIES

Internal Third Parties

Other companies in the Lush Group, acting as joint controllers or processors and who are based in:

Austria

Germany

Hungary

Italy

Sweden

France

Portugal

Spain

Czech

Holland

Luxembourg

Belgium

UAE

Hong Kong

Australia

New Zealand

Japan

and provide IT and system administration services and undertake leadership reporting.

External Third Parties

Service providers acting as joint controllers or processors based:

- Kuwait
- Lebanon
- Macedonia
- Saudi
- Slovenia
- Bulgaria
- Ukraine
- Panama
- Mexico
- Thailand
- South Africa
- Oman
- Bahrain

- Singapore

Services providers acting as processors and controllers based:

- Switzerland
- Croatia
- Russia
- Norway
- Chile
- Finland
- Korea
- USA
- Canada

who provide IT and system administration services.

- Professional advisers acting as processors or joint controllers including lawyers, bankers, auditors and insurers who provide consultancy, banking, legal, insurance and accounting services.
- HM Revenue & Customs, regulators and other authorities acting as processors or joint controllers based in the United Kingdom who require reporting of processing activities in certain circumstances.

Other third parties

- Google Analytics
- Google Cloud
- Google Business
- Electio
- MetaPack
- Olark
- MailChimp/Mandrill
- FFW
- Adyen
- PayPal
- Hotjar
- Slack
- Sendgrid
- Cloudflare
- Conversocial
- Booker

- Rackspace
- Crazyegg
- Anchoris
- Zendesk
- Mitingu
- Eventbrite
- Vacancy Filler
- Sorted
- Royal Mail
- DPD
- UPS
- Ethical Consumer
- Sage
- Eventbrite
- Mitingu
- Vacancy Filler
- Fabric.io
- Queueflow

Website Cookies

Our website uses a few main cookies;

We keep a session cookie which is a small file on our server allowing us to distinguish you from other users, so that we can keep a virtual "basket" of the products you add to your shopping cart.

A second cookie detects whether your browser supports JavaScript, this helps us to deliver the best possible experience online whilst using the Lush website.

We also use Google Analytics, which sets a small cookie file on your computer browser. This cookie stores no personal information about you and will keep a track of how you browse our website. We use this anonymous information to help us further improve the shopping experience on our website.

Some of the pages on Lush.co.uk use content embedded from another website, for example YouTube, you maybe sent cookies from these websites. We don’t actually control these cookies and we would recommend that you visit these third parties for more information about their cookies:

Barclaycard SmartPay (our payment provider), YouTube (to view videos), Facebook (to share content) and NOSTO (provide our trending products, articles and ingredients). Crazy Egg (creates heatmaps of visitors on our site)

We don't sell the information collected by cookies, nor do we disclose the information to third parties, except where required by law (for example to government bodies and law enforcement agencies). We treat your information as sensitive and confidential.

V6

If you continue without changing your settings, we'll assume you are happy to accept all cookies on the Lush website.

If cookies aren’t enabled on your device, it will mean that your shopping experience on our website will be limited to browsing and researching. Unfortunately you will not be able to add products to your basket and buy them.