Privacy Policy

Natterbox Limited is committed to protecting your privacy and maintaining the security of any personal information received from you. Natterbox Limited strictly adheres to the requirements of the data protection legislation in the UK and the EU GDPR regulations. We respect and value the privacy of everyone who works for or interacts with us. We only collect and use personal data in ways that are described here, and in a manner that is consistent with our obligations and your rights under the law.

The latest version of this Privacy Policy will be published on www.natterbox.com/privacy/

Change Log

V1.3-20200520

Contents:

1. Definitions and Interpretation

In this Policy, the following terms shall have the following meanings:

Client Data	Personal Data for which Natterbox is the Data Controller as defined in the "GDPR", whether sent to Natterbox by Clients or collected by the "Service" from the Client's customers.
Client-related Data	All data regarding the Client and Client's customers, whether sent to Natterbox by Client or collected by the "Service" from the Client's customers.
Cookie	Means a small text file placed on your computer or device by our Websites when you visit certain parts or use certain features of them. Details of the Cookies used by our websites are set out in the Marketing and Websites section.
Cookie Law	Means the relevant parts of the Privacy and Electronic Communications (EC Directive) Regulations 2003.
Data Subject	The legal or natural person existing in the "EU" at the time of data collection or "Processing" regarding them.
EU	The European Union and all Third Countries whose Data Protection standards are covered by an adequacy decision by the European Commission as defined in the "GDPR".
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of individuals with regards to the processing of "personal data" ("General Data Protection Regulation"), and any replacement or supplementary directive imposing equivalent obligations.
Group Company	Means any corporation, company, or other legal entity that owns Natterbox or in which Natterbox (or Natterbox's owners) owns or controls, directly or indirectly, more than 50% (fifty percent) of the unrestricted shares entitled to vote for the election of directors or other persons performing similar functions. Parties may deem a company, firm or legal entity, which does not meet the criteria above a Natterbox Affiliate if mutually agreed upon in writing.
Master Agreement	The Master Services Agreement or Subscription Services Agreement entered into by Natterbox and Client for the provision of services.
Personal Data	Means any and all data that relates to an identifiable person who can be directly or indirectly identified from that data. This includes any information relating to a Data Subject which can be accessed by or is disclosed to Natterbox including personal data that you provide to Natterbox via websites, marketing, business functions or products and services. This definition shall, where applicable, incorporate the definitions provided in the EU Regulation 2016/679 – the General Data Protection Regulation ("GDPR").
Personal Data Breach	Means 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 as defined by the GDPR.
Processing	Means any operation which is performed upon Personal Data, including without limitation accessing, collecting, storing, using, organising, combining, altering, transferring, disclosing, transmitting, disseminating or deleting Personal Data, carried out by Natterbox in the course of its activities on behalf of Client or in the course of rendering its services to Client. Processing has the meaning given to it in the GDPR, and "data processing", "process", "processes" and "processed" will be interpreted similarly.
Service(s)	All business operations performed by Natterbox and the supply and connection of services to be performed by Natterbox.
Sub-Processor(s)	A sub-contractor or supplier of Natterbox with respect to Services provided by Natterbox, as defined in the GDPR Article 28(2) and 28(4).
Supervisory Authority	Means the competent authority that supervises the Data Processing by Client or Natterbox as defined by GDPR. For all UK-based transactions of UK citizen data shall be considered to be the ICO.

2. Information About Us

Natterbox Limited, a limited company registered in England under company number 06968249, whose registered address is No.1 Croydon, Croydon, London, CR0 0XT, UK and whose main trading address is No.1 Croydon, Croydon, London, CR0 0XT, UK. Natterbox is part of a group of Companies, all of which are represented here as the 'Company'.

3. What Does This Policy Cover?

This Privacy Policy applies to all areas of the business where information is gathered, processed and stored about clients, non-clients, staff, contractors, suppliers, partners, investors and business contacts.

Specifically:

- Marketing and Websites
- Customers, Prospects and Suppliers
- Employees and Staff

4. Your Rights under GDPR

4.1. As a data subject, you have the following rights under the GDPR, which this Policy and Natterbox's use of personal data have been designed to uphold:

a. The right to be informed about the collection and use of personal data
b. The right of access to the personal data Natterbox holds about you (more information)
c. The right to rectification if any personal data Natterbox holds about you is inaccurate or incomplete
d. The right to be forgotten – i.e. the right to ask Natterbox to delete any personal data they hold about you
e. The right to restrict (i.e. prevent) the processing of your personal data
f. The right to data portability (obtaining a copy of your personal data to re-use with another service or organisation)
g. The right to object to your personal data being used for particular purposes
h. Rights with respect to automated decision making and profiling

4.2. If you have any cause for complaint about the use of your personal data, please contact Natterbox using the details provided in section 14. If Natterbox is unable to help within a reasonable timeframe, you also have the right to lodge a complaint with the UK's supervisory authority, the Information Commissioner's Office.

4.3. For further information about your rights, please contact the Information Commissioner's Office or your local Citizens Advice Bureau.

Marketing and Websites

Natterbox maintain a number of websites and systems for product marketing, advertising, access to products and services, customer support, system information and other business purposes. This Privacy Policy is published on www.natterbox.com.

4.4. Your understanding and acceptance of this Privacy Policy is deemed to occur upon initial and continued use of our web sites and systems. If you do not accept and agree with this Privacy Policy, you must stop using our web sites and systems immediately.

The Information We Collect

4.5. Depending upon your use of our websites, we may collect some or all of the following personal and non-personal data (please also see section 5.4 below on our use of Cookies and similar tracking technologies):

a. Email Address
b. First Name
c. Last Name
d. Company
e. Job Title
f. Street Address
g. City
h. County
i. Postcode
j. Phone Number
k. The type of enquiry your making, including special requirements
l. The information you provide relating to your enquiry
m. Organisation details
n. Details of your referrer
o. Network Provider
p. Telephony Provider
q. IP address
r. Web browser type and version
s. Operating system
t. A list of URLs starting with a referring site, your activity on our websites, and the site you exit to

4.6. Our websites may contain links to other websites. Please note that we have no control over how your data is collected, stored, or used by other websites and we advise you to check the privacy policies of any such websites before providing any data to them.

How The Information Is Collected

4.7. Our websites may place and access certain first party Cookies on your computer or device. First party Cookies are those placed directly by us and are used only by us. We use Cookies to facilitate and improve your experience and to provide and improve our products and services. We have carefully chosen these Cookies and have taken steps to ensure that your privacy and personal data is protected and respected at all times.

4.8. By using our websites you may also receive certain third party Cookies on your computer or device. Third party Cookies are those placed by websites, services, and/or parties other than us. Third party Cookies are used on our websites to better provide a targeted experience for the user. For more details, please refer to section 6, above, and to section 13.6 below. These Cookies are not integral to the functioning of our websites and your use and experience will not be impaired by refusing consent to them.

4.9. All Cookies used by and on our websites are used in accordance with current Cookie Law.

4.10. Before Cookies are placed on your computer or device, you will be shown a message requesting your consent to set those Cookies. By giving your consent to the placing of Cookies you are enabling us to provide the best possible experience and service to you. You may, if you wish, deny consent to the placing of Cookies; however certain features may not function fully or as intended.

4.11. Certain website features depend on Cookies to function. Cookie Law deems these Cookies to be "strictly necessary". These Cookies are shown below. Your consent will not be sought to place these Cookies, but it is still important that you are aware of them. You may still block these Cookies by changing your internet browser's settings as detailed below, but please be aware that our websites may not work properly if you do so. We have taken great care to ensure that your privacy is not at risk by allowing them.

4.12. The following first party Cookies may be placed on your computer or device:

NAME OF COOKIE	PURPOSE	STRICTLY NECESSARY
cookie_consent	This cookie remembers if the cookie notification message has been accepted so it only shows once.	Yes
referer_tracking	Used to track where site users came to the site from, to measure the success of our online marketing campaigns.	No
direct_tracking	Used to track where site users came to the site from, to measure the success of our online marketing campaigns.	No

wordfence_verifiedHuman	Cookie set by the Wordfence Security WordPress plugin to protect the site against malicious attacks.	Yes
wfvt_*	Cookie set by Wordfence Security WordPress plugin, contains information about your general geographic location, used to protect the site against malicious attacks.	Yes

4.13. The following third party Cookies may be placed on your computer or device:

NAME OF COOKIE	PROVIDER	PURPOSE
BizoID	Linkedin	The BizoID cookie stores a unique LinkedIn user ID.
bcookie, bscookie	Linkedin	Used by the social networking service, LinkedIn, for tracking the use of embedded services.
UserMatchHistory	Linkedin	This cookie stores the last time cookie IDs were synced with a given authorized network partner and is part of LinkedIn's server-to-server data integration solution.
lang	Linkedin	Used for LinkedIn integration functionality.
lidc	Linkedin	Used by the social networking service, LinkedIn, for tracking the use of embedded services.
pardot, dtCookie, visitor_id*, visitor_id*-hash	Pardot	We use Pardot to manage our contacts database. These cookies are set to enable us to provide contact forms that link with Pardot systems.

4.14. Our websites use analytics services provided by Google and Facebook. Website analytics refers to a set of tools used to collect and analyse anonymous usage information, enabling us to better understand how our websites are used. This, in turn, enables us to improve our websites and the products and services offered through them. You do not have to allow us to use these Cookies, however whilst our use of them does not pose any risk to your privacy or your safe use of our websites, it does enable us to continually improve our websites, making them better and a more useful experience for you.

4.15. The analytics service(s) used by our websites use Cookies to gather the required information.

4.16. The analytics service(s) used by our websites use the following Cookies:

NAME OF COOKIE	FIRST / THIRD PARTY	PROVIDER	PURPOSE
_ga	Third Party	Google	This cookie is set and used by Google to distinguish users.

_gat	Third Party	Google	Used to distinguish users
_gid	Third Party	Google	Used to distinguish users

Where Is Data Stored And Processed

4.17. We use a number of cloud suppliers as processors of your data and some or all of your data may be processed outside of the EU. Web and marketing sub-processors include:

a. Salesforce CRM and applications
b. Marketing Automation tools
c. Wordpress and web site management tools
d. Content Distribution Networks
e. Advertising and tracking systems including Google

4.18. Where we transfer any personal data outside the EU, we will take all reasonable steps to ensure that your data is treated as safely and securely as it would be within the UK and under the GDPR. You are deemed to accept and agree to this by using our websites and submitting information to us. If we do store data outside the EU, we will take all reasonable steps to ensure that your data is treated as safely and securely as it would be within the UK and under the GDPR including:

a. Ensuring suppliers and sub-processors procure that regulatory requirements applicable in respect of such transfer or access are fully complied with, e.g., when applicable, that such transfer or access is subject to the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.
b. Ensuring suppliers and sub-processors are under data protection obligations consistent with Customer and Supplier Data Processing Agreements and GDPR law.

Who Has Access To Your Information

4.19. Website and marketing data is used only by Natterbox and selected partners for the provision of Natterbox's business services only. Personal Data is not sold or transferred to third parties for other marketing purposes.

4.20. In addition to your rights under the GDPR, set out in section 4, when you submit personal data via our websites you will be given options to restrict use of your data. In particular, we aim to give you strong controls on the use of your data for direct marketing purposes (including the ability to opt-out of receiving emails from us which you may do by unsubscribing using the links provided in emails or via our preference centre online).

4.21. You may also wish to sign up to one or more of the preference services operating in the UK: The Telephone Preference Service ("the TPS"), the Corporate Telephone Preference Service ("the CTPS"), and the Mailing Preference Service ("the MPS"). These may help to prevent you receiving unsolicited marketing. Please note, however, that these services will not prevent you from receiving marketing communications that you have consented to receiving.

4.22. You may access certain areas of our websites without providing any data at all, however, to use all features and functions you may be required to submit or allow for the collection of certain data.

4.23. You may restrict our use of Cookies.

When We Will Use Your Personal Information

4.24. All personal data is processed and stored securely, for no longer than is necessary in light of the reason(s) for which it was first collected. We will comply with our obligations and safeguard your rights under the GDPR at all times. For more details on security see Disclosure/Data Sharing (5.3 below).

4.25. Our use of your personal data will always have a lawful basis, either because it is necessary for our performance of a contract with you, because you have consented to our use of your personal data (e.g. by subscribing to emails), or because it is in our legitimate interests.

4.26. We may use your marketing and website data for the following purposes:

a. Personalising and tailoring your experience on websites
b. Analysing your use of our websites and gathering feedback to enable us to continually improve and enhance your user experience;
c. Surveys and market research
d. With your permission and/or where permitted by law, We may also use your data for marketing purposes by supplying you with information and emails that you have opted-in to (you may unsubscribe or opt-out at any time by clicking unsubscribe links or visiting our preference centre via our website). This may include contacting you by email, telephone, text message and post with information, news and offers about our products and services. We will not, however, send you any unsolicited marketing or spam and will take all reasonable steps to ensure that we fully protect your rights and comply with our obligations under the GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

4.27. Third parties (including Pardot and Salesforce) whose content appears on Our Site may use third party Cookies, as detailed below. Please refer to this section (5.27) for more information on controlling Cookies. Please note that We do not control the activities of such third parties, nor the data they collect and use and advise you to check the privacy policies of any such third parties.

4.28. You have the right to withdraw your consent to us using your personal data at any time, and to request that we delete it.

4.29. We only keep your personal data for as long as we need to in order to use it as described above, and/or for as long as we have your permission to keep it.

4.30. In addition to the controls that we provide, you can choose to enable or disable Cookies in your internet browser. Most internet browsers also enable you to choose whether you wish to disable all cookies or only third party Cookies. By default, most internet browsers accept Cookies but this can be changed. For further details, please consult the help menu in your internet browser or the documentation that came with your device.

4.31. You can choose to delete Cookies on your computer or device at any time, however you may lose any information that enables you to access our websites more quickly and efficiently including, but not limited to, login and personalisation settings.

4.32. It is recommended that you keep your internet browser and operating system up-to-date and that you consult the help and guidance provided by the developer of your internet browser and manufacturer of your computer or device if you are unsure about adjusting your privacy settings.

Disclosure/Data Sharing

4.33. Data security is very important to us, and to protect your data we have taken suitable measures to safeguard and secure data collected through our websites and systems, including:

a. Physical access controls - using GDPR compliant suppliers
b. Media protection and controls - encryption and physical protection
c. Storage controls - ensuring the data and systems are secure and protected against unauthorised access
d. Data access controls - encrypting and securing data and restricting access to authorised personnel only
e. Data transmission controls - serving websites securely, posting form data over SSL, protecting infrastructure and systems against malware and vulnerabilities
f. Data reliability and recovery controls - ensuring redundancy and resilience in systems, people, processes and data.

4.34. Natterbox does not sell, rent or exchange your personal information with any third party for commercial reasons.

4.35. We may compile statistics about communications and the use of systems and websites including data on traffic, usage patterns, user numbers, sales, and other information. All such data will be anonymised and will not include any personally identifying data, or any anonymised data that can be combined with other data and used to identify you. We may from time to time share such anonymised data with third parties such as prospective investors, affiliates, partners, and advertisers. Data will only be shared and used within the bounds of the law.

4.36. In certain circumstances, we may be legally required to share certain data held by us, which may include your personal data, for example, where we are involved in legal proceedings, where we are complying with legal requirements, a court order, or a governmental authority.

5. Customers, Prospects and Suppliers

This section covers how Natterbox collects, uses, stores and discloses the data that other organisations provide to it whilst conducting business activities. It applies to customers, prospects, partners, ex-customers, suppliers, ex-suppliers, business contacts and other external agencies.

Natterbox has a detailed and separate *Customer Data Processing Agreements* and *Supplier Data Processing Agreements* which fully describe our Privacy and Data Protection policies, Technical and Organisational Measures and Data Processing Details according to GDPR requirements and privacy law. Copies are available for customers or suppliers.

The following provides a summary of the key privacy components:

The Information We Collect

5.1. Business communications and correspondence including emails, instant messaging, social media, telephone, post, fax, chat and other online and physical interactions.

5.2. Contact and business information about you and your organisation

5.3. Information about you and your organisation that helps us understanding your organisation and business needs

5.4. Information required to supply products and services to you and your organisation

5.5. Information related to the supply of goods and service from you and your organisation.

5.6. Contractual and legal information about you and your organisation

5.7. Information required to perform financial activities with you and your organisation

5.8. Information required for facilitating, personalising and tailoring our products and services for you

5.9. Information about your usage of our products and services

5.10. Information about our use of your organisation's products and services

5.11. Information required to maintain and support our products, services and systems

5.12. Information required to maintain and support the use of your products, services and systems

How The Information Is Collected

5.13. Natterbox collect information through communications, CRMs, online portals, online communities, business intelligence systems, financial systems, ERP systems and normal business activities and processes, either directly from you and your organisation or via business databases, online services (LinkedIn, D&B etc) or other external credit, legal, reference or other agencies.

5.14. We collect additional personal information in the course of business-related activities throughout the period of you using our products and services.

5.15. We collect additional personal information in the course of business-related activities throughout the period of us using your products and services.

5.16. Natterbox store and process Personal Data only upon your or your organisation's instructions. Natterbox, suppliers and sub-processors shall at all times comply with applicable privacy regulations on the protection of Personal Data in all relevant countries to the extent that they apply for the duration of the business relationship.

Where Is Data Stored And Processed

5.17. The following activities are carried out by Natterbox and third-party service providers in the course of normal business services:

a. IT and Communications services
b. CRM functions
c. Business services
d. Marketing functions
e. Financial control and analysis
f. Legal advisory services

5.18. Business information is stored and processed using a number of cloud based systems, including, but not limited to:

a. Salesforce CRM and associated applications
b. Marketing automation tools
c. Electronic contract and signature systems
d. Financial and accounting systems
e. File storage systems
f. Cloud business services for document production and information processing
g. Business information management systems
h. Communications systems

5.19. All suppliers, services and systems are reviewed and assessed according to their data protection, privacy policies and GDPR compliance status. This assessment is performed according to Natterbox's Cloud Security Policy and Supplier Review and Data Processing Agreements.

Who Has Access To Your Information

5.20. We ensure ourselves, our suppliers and sub-processors have in place and at all times and shall maintain the appropriate operational and technological processes and procedures to protect Personal Data as required by applicable Privacy Regulations, in particular to safeguard the Personal Data against any unlawful or unauthorised access, loss, destruction, theft, use or disclosure.

5.21. We ensure ourselves, our suppliers and sub-processors shall keep Personal Data confidential. This obligation is perpetual. Natterbox makes available Personal Data to its employees, suppliers and sub-processors on a strict need to know basis and obliges all employees, suppliers and sub-processors with access to Personal Data to the secrecy of Personal Data in writing.

When We Will Use Your Personal Information

5.22. Natterbox, suppliers and sub-processors shall only use the Personal Data for the purpose of performance of normal business activities and services agreed. Personal Data shall not be used for any other purposes than those related to business activities or services agreed, except where otherwise authorised or consented to by Natterbox in writing, including but not limited to the use of Personal Data for direct marketing purposes or solicitations by suppliers or any third parties.

Disclosure/Data Sharing

5.23. We may have to share your data with third parties, including third-party service providers (including clients, contractors, suppliers, sub-processors and designated agents); other entities in the group; in the context of business operations; or with a regulator or to otherwise comply with the law; our insurers and/or professional advisers to manage risks and legal disputes.

5.24. We share data where required by law; where it is necessary to administer the working relationship with you; or where we have another legitimate interest in doing so.

5.25. We require third parties to respect the security of your data and to treat it in accordance with the law.

Transfers Of Data Outside Of The EU

5.26. We use a number of Cloud-based file storage and processing systems, many of which are global in nature. Where possible, we ensure processing is performed in the EU. We may transfer the personal information we collect about you outside the EU as part of normal business activities in order to provide services and perform our contract with you.

5.27. Where such transfer occurs, Natterbox, suppliers and sub-processors procure that regulatory requirements applicable in respect of such transfer or access are fully complied with, e.g., when applicable, that such transfer or access is subject to the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

5.28. Natterbox and its suppliers ensures that any sub-processor is under data protection obligations consistent with Customer and Supplier Data Processing Agreements and GDPR law.

Data Retention

5.29. Natterbox, suppliers and sub-processors shall keep Personal Data for no longer than necessary and when required delete it data securely from all systems to prevent further access or use.

5.30. Personal Data related to marketing information is maintained for a maximum of two (2) years.

5.31. Financial records are maintained for a minimum of seven (7) years.

5.32. Customer and supplier information is maintained for the duration of the business relationship and then for up to three (3) years afterwards. Non-personal information about ex-customers, ex-partners and ex-suppliers is maintained on the CRM indefinitely.

5.33. Customer call logs and telephone call records are maintained indefinitely according to national and international Telecommunication and security regulations.

5.34. Personal data used for long term business performance, product metrics and system statistics will be anonymised before use.

6. Employees and Staff

This policy covers how we collect, use, store and disclose the data that staff and contractors supply to us and your rights about data that we hold about you. It applies to current and former employees, job candidates, workers, volunteers, interns, apprentices and contractors and does not form part of any contract of employment or other contract to provide services.

Natterbox and Red Matter (Group Companies) are committed to protecting the privacy and security of your personal information and we will always treat you and your data with the respect you deserve.

The Information We Collect

6.1. Personal individual 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). A table summarising the personal information we collect and hold, how and why we do so, how we use it and with whom it may be shared is below.

6.2. We use information about you primarily to allow us to perform our contract with you and to enable us to comply with legal obligations to provide recruitment, HR, payroll and employment services.

6.3. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties provided your interests and fundamental rights do not override those interests.

6.4. Recruitment information is gathered and maintained for the purposes of deciding whether you are sufficiently qualified, experienced and suitable for job roles. Recruitment information is only shared between staff directly involved in the recruitment process.

6.5. We seek to ensure that our personal information collection and processing is always proportionate. We will notify you of any material changes to personal information we collect or to the purposes for which we collect and process it.

How The Information Is Collected

6.6. We collect personal and professional information through the application process, during recruitment, by the onboarding processes and throughout the period of you working for us.

6.7. Information is collected either directly from candidates or staff or sometimes from external agencies. We may sometimes collect additional information from third parties including former employers or other background check and credit reference agencies.

Where Is Your Data Stored And Processed

6.8. Personal information may be held at our offices and third-party agencies, service providers, representatives and agents as described and in cloud-based IT services. In the event that we use cloud based IT services, personal information may be transferred internationally to other countries around the world, including countries that do not have data protection laws equivalent to those in the UK. We have security measures in place to seek to ensure that there is appropriate security for personal information we hold.

6.9. Natterbox, suppliers and sub-processors shall at all times comply with applicable privacy regulations on the protection of Personal Data in all relevant countries to the extent that they apply for the duration of the business relationship.

6.10. Applicant, employee and HR data is stored and processed using a number of cloud based systems, including:

a. Applicant tracking systems
b. Candidate screening and testing systems
c. Cloud business services for document production and information processing
d. Electronic contract and signature systems
e. File storage systems
f. HR record keeping systems
g. Financial, payroll, banking and accounting systems
h. Business information management systems
i. Associated benefit provider systems
j. Expense tracking systems
k. Disclosure and Reference agency systems
l. Communications systems

6.11. All suppliers, services and systems are reviewed and assessed according to their data protection, privacy policies and GDPR compliance status. This assessment is performed according to Natterbox's Cloud Security Policy.

Who Has Access To Your Information

6.12. We ensure ourselves, our suppliers and sub-processors keep Personal Data confidential. This obligation is perpetual. Natterbox makes available Personal Data to relevant employees, suppliers and sub-processors on a strict need to know basis and obliges all employees, suppliers and sub-processors with access to Personal Data to the secrecy of Personal Data in writing.

6.13. We ensure ourselves, our suppliers and sub-processors have in place and at all times and shall maintain the appropriate technological and organisational measures to protect Personal Data as required by applicable Privacy Regulations, in particular to

safeguard the Personal Data against any unlawful or unauthorised access, loss, destruction, theft, use or disclosure.

6.14. Personal information may be shared with other parties, such as group companies and/or affiliated companies, external contractors and our professional advisers (e.g. legal and financial advisors), HR advisors and payroll providers, and potential purchasers of some or all of our business or on a restructuring. The recipient of the personal information will be bound by confidentiality obligations. We may also be required to share some personal information to comply with the law.

6.15. Data category and access:

a. Role and Job descriptions - HR, relevant departmental manager and senior managers, candidates and staff
b. Applicant information - HR, relevant departmental manager and senior managers
c. Job Offers and Contracts - HR, finance, relevant departmental manager and senior managers
d. Salary and Payroll - HR, finance, relevant departmental manager and senior managers
e. Disciplinary and performance reviews - HR, finance, relevant departmental manager and senior managers
f. Dismissal and off-boarding - HR, finance, relevant departmental manager and senior managers

When We Will Use Your Personal Information

6.16. We collect and use all the categories of information identified below as necessary to allow us to perform our contract with you and to enable us to comply with legal obligations and Company policies. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties provided your interests and fundamental rights do not override those interests. We will collect and process personal information as follows:

Information we Collect	How we Collect the information	Why we Collect the Information (including legitimate interest)	How we May Use the Information	How we May Share the Information
Personal contact details such as your name, address, telephone, email, emergency contacts, etc *	From you From recruitment agencies acting on your behalf	Contract, Empl. Records, Benefits, Recruitment	Contract, Staff Admin, Recruitment	HR & Admin, Benefits

Personal details such as next of kin, marital status, dependants, sex, date of birth etc *	From you	Contract, Empl. Records, Benefits	Contract, Staff Admin	HR & Admin,
Financial details such as bank information, salary, benefits, national ID, tax information, etc *	From you	Contract, Empl. Records, Benefits	Contract	HR & Admin, HMRC, Bank, Benefits
Your skills, qualifications and any professional status *	From you, from recruitment agencies acting on your behalf	Contract, Empl. Records, Recruitment	Contract, Staff Admin, Training	HR & Admin, Clients (if required)
Recruitment information including application details, interview notes, screening notes, screening videos and telephone calls, capability test results and notes, references, recruitment information	From you, from recruitment agencies acting on your behalf	Recruitment	Contract, Staff Admin	HR & Admin
Your nationality and immigration status, right to work, visas and information from related documents (e.g. passport) *	From you, the Home & Immigration Offices Ofice (if required)	Contract, Empl. Records	Contract	HR & Admin, Home & Immigration Offices, Visa applications (if required)
Driving licence details (if required by your role or for Company vehicles) *	From you, the DVLA portal	Contract, Empl. Records, Insurance	Contract, Insurance, Staff Admin, Benefits	HR & Admin, Insurers, Driving history reference agencies
Pension arrangements and all information necessary to implement and administer them *	From you, pension administrators	Contract, Benefits	Contract, Staff Admin	HR & Admin, Pension administrators, HMRC & Tax authorities
Sickness, injury and absence records (including sensitive personal information regarding your physical and/or mental health) *	From you, Medical Professionals, any insurance benefit administrators	Contract, Empl. Records, Safe Working	Contract, Legal, Staff Admin, Access, Safe Working	HR & Admin, Medical Professionals, Insurance
Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs	From you	Not recorded or used unless required in a dispute or as a Legal requirement	To ensure adherence to company and statutory policies	No-one unless forced
Trade Union (TU) membership	From you, your TU	Contract Empl. Records	Contract	HR & Admin Your TU

Job related information such as role, salary, compensation history, performance, appraisals, disciplinary history, etc. *	From you, other employees, consultants	Contract, Empl. Records, Legal, Policies	Contract, Legal, Staff Admin	HR & Admin
Information on grievances & conduct issues	From you, other employees, consultants, any relevant third parties	Contract, Empl. Records, Legal, Safe Working	Contract, Staff Admin	HR & Admin, Legal, Other relevant third parties (as appropriate)
Leave, attendance records and travel logs and information *	From you, HR Toolkit, Concur	Empl. Records,	Contract, Access, Staff Admin	HR & Admin
Your use of our systems and your actions in and around the workplace	Company devices, Applications, Cloud Services, other systems (e.g. CCTV, access control systems, phone, email, internet)	Contract, Access, Protect, Policies, Operational	Access, Protect, Policies, Operational	HR & Admin, Relevant third parties
Your use of public social media (only in very limited circumstances to check specific risks for specific functions within our organisation) and any business related social media (e.g. LinkedIn)	Websites, Applications	Contract, Protect, Policies, Reputation	Contract, Protect, Policies, Reputation	HR & Admin
Photographs *	From you, the Company or other suppliers requiring ID	Empl. Records, ID documents, Access Control, Marketing, Staff directory and Staff Information Trello Board	Empl. Records, Access, Staff Admin	Marketing material Relevant third parties (ie for supplier/client security)
Details in references about you that we give to others	From your personnel records, other employees	Contract, Legal, Empl. Records	To provide a reference	HR & Admin, The recipient(s) of the reference
Criminal records information, including credit checks and the results of DBS checks *	From you, DBS, credit rating agencies	Contract, Legal	Contract, Legal, Training	HR & Admin, DBS, Supplier/Client security vetting, Other regulatory authorities as required

Key to table above

Access	To monitor/manage staff access to our systems and to record staff absences

Bank	Our banks and payment processors for salaries, expenses and other payments
Benefits	Company benefit providers such as Perkbox, healthcare, pensions etc
Contract	To enter into and perform our contract with you
DBS	Disclosure and Barring Service. Government organisation(s) that can perform background and reference checks including requesting a criminal record certificate, enhanced criminal record certificate or a search of the children's or adults' barred list
Empl. Records	To maintain employment records and for good employment practice
HR & Admin	Relevant managers, HR, professional advisors, payroll and professional HR & Admin consultants
Insurance	To comply with the terms of our insurances
Legal	To ensure compliance with legal and/or regulatory obligations
Medical Professional	Your doctors and other medical/occupational health professionals
Operational	To facilitate resource planning and provision
Policies	To ensure compliance with our policies, such as Equal Opportunities Policy, Sickness absence policies, Corporate Communication and Social Media Policy, Information Security Policies, Privacy Policies, etc
Protect	To protect our networks, intellectual property and personal data of employees, clients and suppliers
Recruitment	To make hiring decisions
Reputation	To ensure staff and Company reputation and good standing
Safe Working	To ensure safe working practices
Staff Admin	To facilitate staff administration, record keeping and Company communications (ie Staff forms, newsletter, staff information)
Training	Internal and external personal development and training

Failure to Provide Information

6.17. If you fail to provide certain information when requested (marked with * above), we may not be able to make an informed and objective decision about your suitability and competency for a role, perform the contract we have entered into with you (such as paying you, providing employee benefits and to administer statutory payments such as statutory sick pay (SSP)), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our staff).

6.18. If you do not provide this information, we may not be able to employ you, make these payments or provide these benefits.

Sensitive Personal Information

6.19. "Special categories" of particularly sensitive personal information require higher levels of protection. We may process special categories of personal information in the following circumstances:

a. In limited circumstances, with your explicit written consent.
b. Where we need to carry out our legal obligations and in line with our Privacy Policy.
c. Where we perform personal security and background checks.
d. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with our Privacy Policy.

e. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

6.20. Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

Our Obligations As An Employer

6.21. We will use your particularly sensitive personal information in the following ways:

a. We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
b. We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
c. Only if required by law, we will anonymise and use information about your race or national or ethnic origin, religious, philosophical or moral beliefs or sexual orientation to ensure meaningful equal opportunity monitoring and reporting. Natterbox **does not** habitually record, monitor or care about these characteristics.

Information About Criminal Convictions

6.22. We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our Privacy Policy.

6.23. We may process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

6.24. We may carry out Disclosure and Barring Service (DBS) checks (including requesting a criminal record certificate, enhanced criminal record certificate or a search of the children's or adults' barred list) where we feel that a DBS check if proportionate and relevant for your role. A record that the DBS check was completed and whether it was satisfactory will be kept; however, the check itself will usually be disposed of securely unless we feel it is relevant to the ongoing employment relationship, in which case it will be kept securely for six months (unless relevant for regulatory inspections in which case it will be retained until the next inspection).

6.25. Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

6.26. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

6.27. We will use information about criminal convictions and offences in the following ways:

a. Disclosure to and decisions about your ability to work within regulated customers such as financial institutions.
b. Disclosure to and decisions about your ability to work within secure sites such as data centres and communications suppliers.
c. Decisions about your ability to work in certain foreign countries.
d. Disclosure to visa and immigration authorities for the purpose of obtaining work visas.
e. Disclosure to employment tribunals or other legal authorities.

Your Duty To Inform Us Of Changes

6.28. It is important that the personal information we hold about you is accurate and current, so please let us know and update your HR records if your information changes.

Disclosure/Data Sharing

6.29. We may have to share your data with third parties, including third-party service providers (including clients, contractors and designated agents); other entities in the group; in the context of a sale of the business; or with a regulator or to otherwise comply with the law; our insurers and/or professional advisers to manage risks and legal disputes.

6.30. The following activities are carried out by third-party service providers: payroll, pension administration, benefits provision and administration, HR advisory services, legal advisory services, IT and Communications services.

6.31. We share data where required by law; where it is necessary to administer the working relationship with you; or where we have another legitimate interest in doing so.

6.32. References will be provided upon request from the ex-member of staff. References shall be verified and will usually only include the party's start date and end date without the disclosure of further personal information.

6.33. We require third parties to respect the security of your data and to treat it in accordance with the law.

Transfers Of Data Outside Of The EU

6.34. We use a number of Cloud-based file storage and processing systems, many of which are global in nature. Where possible, we ensure processing is performed in the EU.

We may transfer the personal information we collect about you outside the EU to enable us to perform our contract with you.

6.35. Where such transfer occurs, Natterbox, suppliers and sub-processors procure that regulatory requirements applicable in respect of such transfer or access are fully complied with, e.g., when applicable, that such transfer or access is subject to the standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

6.36. Natterbox and its suppliers ensures that any sub-processor is under data protection obligations consistent with Customer and Supplier Data Processing Agreements and GDPR law.

Data Retention

6.37. Natterbox, suppliers and sub-processors shall keep Personal Data for no longer than necessary and when required delete it data securely from all systems to prevent further access or use.

6.38. Recruitment interview and application records are retained for 6 (six) months after receipt.

6.39. Basic applicant tracking information (names and role applied for) is retained for two years.

6.40. We may request permission to retain contact details for future opportunities for longer.

6.41. We must store most of your HR data for a period of at least 6 years following the termination of your employment; some personal financial data will be destroyed after 2 years; Health and Safety information must be held for a minimum of 40 years. Pension Information must be retained indefinitely or until you attain pension age.

6.42. Personal data used for long term business performance, product metrics and system statistics will be anonymised before use.

7. What Happens If Our Business Changes Hands?

7.1. We may, from time to time, expand or reduce our business and this may involve the sale and/or the transfer of control of all or part of these businesses. Any personal data that you have provided will, where it is relevant to any part of our business that is being transferred, be transferred along with that part and the new owner or newly controlling party will, under the terms of this Privacy Policy, be permitted to use that data only for the same purposes for which it was originally collected by us. In the event that any of your data is to be transferred in such a manner, you will be contacted in advance and informed of the changes.

7.2. When contacted you will be given the choice to have your data deleted or withheld from the new owner or controller.

8. Your Data Subject and Data Access Rights

8.1. You have the right to ask for a copy of any of your personal data held by us (where such data is held).

8.2. Under the GDPR, no fee is payable and we will provide any and all information in response to your request free of charge.

8.3. Where the information requested is private in nature we may ask for verification of your identity to assess your legal right to access the information.

8.4. Where Natterbox are deemed not to be your Data Controller (ie you did not initially give Natterbox your information, but it was given to a different organisation or customer of Natterbox) we shall request that you redirect your request to that organisation as your Data Controller.

8.5. We aim to provide an acknowledgement of any request within 5 (five) business days

8.6. We shall endeavour to provide the requested information within 30 (thirty) days.

8.7. As a registered Telco, Natterbox is subject to national and international Telecommunications laws and regulations that require client records and call logs to be maintained for security and regulatory purposes. This means that some deletion requests may not be possible.

8.8. Information requested will be provided electronically in a secure and easily accessible format.

8.9. We will maintain a record of your Subject access request for 2 (two) years.

8.10. Please contact us for more details at **privacy@natterbox.com**, or using this Subject Access Request form.

9. Contacting Us

9.1. If you have any questions about this Privacy Policy or how we handle your personal information, please contact the person responsible for Data Protection in our Company. If we have breached our duty of care, we will take appropriate action.

9.2. Please contact us:

a. by email at privacy@natterbox.com,
b. by telephone on +44 203 510 0500, or
c. by post at No.1 Croydon, Croydon, London, CR0 0XT, UK.

9.3. You will be asked to provide specific written information and instructions about your request. We may also ask you to verify your identity. Where we are not your Data Controller we shall refer you to the relevant organisation to deal with your request.

9.4. If you are not satisfied by our response you also 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 (Email: casework@ico.org.uk)

10. Changes to Our Privacy Policy

10.1. We may change this Privacy Policy from time to time (for example, if the law changes or suppliers or business processes change). Any changes will be immediately posted on our websites and you will be deemed to have accepted the terms of the Privacy Policy on your first use of these sites following the alterations. We recommend that you check our privacy policy pages and documents regularly to keep up-to-date.

Change Log

10.2. The following table contains a list of revisions and changes

Date	Version	Change history	Modified by
21 May 2018	1.21	Initial published version	AE
23 May 2018	1.22	Corrections and revisions	AE, TB, TR, NB, MAV, HR, SW
10 June 2018	1.23	Updated and revised Employees and Staff section. Updated the Where is Data Stored and Processed section Updated Contacting Us section Added Change Log	AE, HR
15 July 2019	1.24	Annual review	AE
20 MAy 2020	1.3	Annual review and ISO27001 Audit DSAR link update	AE, LF