PRIVACY POLICY

Last Updated: July 2023

1. INTRODUCTION

At Delice de France, we regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business.

We are committed to safeguarding the privacy and security of our customers and website visitors' personal data; this policy sets out how we will treat your personal information including any data that is provided to us:

- when you are visiting our sites or via associated applications when opening the account
- when you access and browse our website
- when you contact us through the website or via other means

Our website uses cookies. By using our website and agreeing to this policy, you consent to our use of cookies in accordance with the terms of this policy. We created this privacy policy solely for the purposes of practice at Delice de France Ltd.

By using the Site, you agree to the collection and data processing in accordance with this Privacy Policy. It is important that you read this Privacy Policy 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.

2. DEFINITIONS

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

3. INFORMATION DO WE COLLECT

We may collect, store, and use the following kinds of information:

- Contact information (e.g., name, address, email address, phone number) including information that you provide to us for the purpose of registering with us
- Company details (e.g., company name, registration number)
- Billing and payment information including information relating to any transactions carried out between you and us on or in relation to this website and relating to any purchases you make of our goods or services
- Trading relationship details (e.g., direct customer, distributor, buying group relationship)
- Credit-related information for credit reference checks

- Information about your computer and about your visits to and use of this website (including your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views, website navigation and details);
- Information that you provide to us for the purpose of subscribing to our website services, email notifications and/or newsletters (including details);
- Any other information that you choose to send to us; and other information.

We also collect, use, and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example, we may aggregate your Usage Data to calculate the percentage of users accessing a specific Site 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 that will be used in accordance with this Privacy Policy.

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.

4. HOW WE COLLECT YOUR PERSONAL DATA

- Direct Interactions: You may provide us with your personal data when contacting us through the Website or signing up as a new customer. You can give us your Profile Data and Identity and Contact Data when registering and using our career opportunities feature. You may also provide us with your personal data when corresponding with us by post, phone, email or otherwise.
- Automated technologies or interactions. As you interact with the Website, we collect technical data and usage data.

5. PURPOSE AND LEGAL BASIS FOR PROCESSING YOUR PERSONAL INFORMATION

We process personal data for the following purposes and based on the corresponding legal bases:

5.1 Performance of a Contract:

- To provide requested products or services
- To manage and maintain business relationships.
- To process orders, invoices, and payments

5.2 Compliance with Legal Obligations:

- To fulfil legal, accounting, and reporting requirements
- To comply with applicable laws, regulations, and governmental requests

5.3 Legitimate Interests:

- To communicate with individuals about products, services, and promotions.
- To respond to inquiries, complaints, or requests for support.

- To conduct market research and improve our products and services.
- To prevent and detect fraud or other illegal activities.
- To protect our rights, property, and safety, as well as the rights, property, and safety of individuals and others.

5.4. Credit Reference Checks:

- To assess creditworthiness and manage credit-related risks.
- To conduct credit reference checks with relevant credit reference agencies
- If you have applied for credit, as part of the credit assessment process, we will perform credit and identity checks on you at your business address. These checks are essential for processing your credit application and determining your creditworthiness.
- To conduct the credit reference checks, we may share your personal data, including your name, business address, and other relevant information, with credit reference agencies. These agencies are independent organisations that specialise in assessing creditworthiness and maintaining credit-related information.
- The credit reference agencies will use the provided information to verify your identity, assess your credit history and financial standing, and generate a credit report that helps us evaluate your creditworthiness. The credit report may include details such as your credit score, previous credit applications, outstanding debts, and payment history.
- Credit reference checks are conducted in compliance with applicable data protection laws and regulations. We have implemented appropriate safeguards to protect the confidentiality and security of your personal data throughout the credit assessment process. We only share the necessary information required for the credit reference agencies to perform their assessment.

5.5. Monitoring of Communications:

Subject to applicable laws, we may monitor and record your calls and emails in relation to your dealings with us. We undertake these monitoring activities for various purposes, including:

- Compliance and Self-Regulatory Practices: We monitor communications to ensure compliance with applicable laws, regulations, and industry standards. This helps us maintain high standards of service and conduct.
- Crime Prevention and Detection: Monitoring communications allows us to prevent and detect fraudulent activities, unauthorised access, and other potential threats to our systems and operations.
- Security of Communications Systems and Procedures: We monitor communications to protect the security and integrity of our communication systems, networks, and procedures. This helps us identify and address any vulnerabilities or breaches.
- Content Moderation: We monitor communications to identify and prevent the transmission of obscene or profane content. This is done to maintain a safe and respectful environment for all parties involved.
- Quality Control and Staff Training: Monitoring communications helps us ensure the quality of our services and provides valuable insights for staff training and development. This enables us to continuously improve our customer service and support.

- Record-Keeping: We may need to maintain records of your communications to have a comprehensive record of what has been discussed or agreed upon. This is particularly important for resolving disputes, addressing inquiries, or meeting legal requirements.
- We may monitor activities on your account, when necessary, for the aforementioned reasons. Such monitoring is justified by our legitimate interests in maintaining the security and integrity of our services and systems, as well as fulfilling our legal obligations.

5.6 Managing online presence

- Administer the website.
- Improve your browsing experience by personalising the website.

Where you submit personal information for publication on our website, we will use that information in accordance with the license you grant to us. We will not without your express consent provide your personal information to any third parties for the purpose of direct marketing.

6. TRACKING & COOKIES DATA

We use cookies and similar tracking technologies to track the activity on our website and hold certain information.

Cookies are files with a small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Tracking technologies also used are beacons, tags, and scripts to collect and track information and to improve and analyse our Site. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Site.

Examples of Cookies we use:

- Session Cookies. We use Session Cookies to operate our Site.
- Preference Cookies. We use Preference Cookies to remember your preferences and various settings.

Security Cookies. We use Security Cookies for security purposes.

7. DISCLOSURES

We may disclose information about you and your personal information, to the extent that we are required to do so by law. In connection with any legal proceedings or prospective legal proceedings. In order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk).

- To internal third parties: In the event of a merger, acquisition, or sale of assets, personal data may be transferred to the relevant parties involved. We will take appropriate measures to ensure the protection of personal data during such transactions.
- To Credit Reference Agencies: For the purpose of conducting credit reference checks, we may share personal data with credit reference agencies and obtain credit reports.
- The provision of and administration of the website. Ensuring your queries are directed to the correct entity, and (iii) ensuring your career opportunity queries are shared with relevant recruitment persons within the business. To external third parties: Companies that provide products and services to us such as professional advisors, IT service providers, data storage

solutions, IT developers, insurance providers, analytics companies, website hosting providers, payment processors and logistics partners and other service providers. These service providers are contractually obligated to process personal data only in accordance with our instructions and for the purposes specified by us.

Except as provided in this privacy policy, we will not provide your information to third parties. We require all third parties to whom we disclose personal data to respect the security of personal data and to treat it in accordance with the law. We do not allow our service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions. Unless prevented by applicable law, we will notify you when your personal data may be provided to third parties in ways other than explained above, and you may have the option to prevent such sharing at the time that we notify you.

8. YOUR LEGAL RIGHTS

Under certain circumstances, you have rights under data protection laws in relation to your personal data as follows:

- Request access to your personal data. 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 your personal data. 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 the 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, 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 your personal data. This enables you to ask us to suspend the processing of your personal data: (i) if you want us to establish the data's accuracy; (ii) where our use of the data is unlawful but you do not want us to erase it; (iii) 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 (iv) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.
- Request transfer of your personal data. 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.
- Right to 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.

If you wish to exercise any of the rights set out above, please contact us at HRinbox@ddf.co.uk. 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 could refuse to comply with your request in these circumstances.

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.

If you would like to access your data, you should make a Subject Access Request. Further information on making a subject access request is contained in our Subject Access Request policy. We will comply with the request within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit. Please note that the maximum length of the extension that can be granted is equal to two months.

If you would like a copy of the information held on you, please write to, Delice de France Ltd, Delice House, 149 Brent Road, Southall, Middlesex UB2 5LJ.

If you believe that any information, we are holding on you is incorrect or incomplete, please write to or email us as soon as possible, at webshop@ddf.co.uk. We will promptly correct any information found to be incorrect upon the successful identity verification.

We try to respond to all legitimate requests within one month. Occasionally it could 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.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator 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.

9. INTERNATIONAL TRANSFERS

The Company does not transfer personal data to any recipients outside of the EEA.

10. CONTROLLING PERSONAL INFORMATION

We will not sell, distribute, or lease your personal information to third parties unless we have your permission or are required by law to do so. You may choose to restrict the collection or use of your personal information in the following ways:

- Whenever you are asked to fill in a form on the website, look for the box that you can click to indicate that you do not want the information to be used by anybody for direct marketing purposes.

- If you have previously agreed to us using your personal information for direct marketing purposes, you may change your mind at any time by emailing us at webshop@ddf.co.uk. Alternatively, click on the unsubscribe link in marketing emails from us to unsubscribe.

11. SECURITY OF PERSONAL INFORMATION

We take appropriate technical and organisational precautions to protect personal data against unauthorised access, prevent the loss, misuse, or alteration of your personal information. We store all the personal information you have consented to provide us on our secure (password and firewall protected) servers. All electronic transactions you make to or receive from us will be encrypted. Data transmission over the internet is inherently insecure, and we cannot guarantee the security of data sent over the internet.

You are responsible for keeping your password and user details confidential. We will not ask you for your password (except when you log in to the website). We regularly assess and update our security measures to address new risks and ensure the ongoing confidentiality, integrity, and availability of personal data.

12. REQUIREMENT TO NOTIFY BREACHES

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach. More information on breach notification is available in our Breach Notification policy.

13. RETENTION

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

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, regulatory, tax, accounting, or other requirements.

By law, we have to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they cease being customers for tax purposes.

In some circumstances, we will anonymise your personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

14. POLICY AMENDMENTS

We may update this privacy policy from time-to-time by posting a new version on our website. You should check this page occasionally to ensure you are happy with any changes.

We may also notify you of changes to our privacy policy by email. This policy was last updated in July 2023.

15. THIRD PARTY WEBSITES

Our Site may contain links to third-party sites that are not operated by us. If you click on a third-party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third-party sites or services.

16. DATA CONTROLLER

The data controller responsible in respect of the information collected on this website is Delice de France Ltd.

17. CONTACT

If you have any questions about this privacy policy or our treatment of your personal information, please write to us by email at HRinbox@ddf.co.uk or by post to Delice de France Ltd, Delice House, 149 Brent Road, Southall, Middlesex UB2 5LJ.

SUBJECT ACCESS REQUEST POLICY

Last Updated: June 2023

1. INTRODUCTION

You have a right, under the General Data Protection Regulation, to access the personal data we hold on you. To do so, you should make a subject access request, and this policy sets out how you should make a request, and our actions upon receiving the request.

2. DEFINITIONS

“Personal data” is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including your name.

“Special categories of personal data” includes information relating to:

a) Race
b) Ethnic origin
c) Politics
d) Religion
e) Trade union membership
f) Genetics
g) Biometrics (where used for id purposes)
h) Health

i) Sex life or
j) Sexual orientation.

3. MAKING A REQUEST

Although subject access requests may be made verbally, we would advise that a request may be dealt with more efficiently and effectively if it is made in writing. If you wish to make a request, please use the Subject Access Request form.

Requests that are made directly by you should be accompanied by evidence of your identity. If this is not provided, we may contact you to ask that such evidence be forwarded before we comply with the request.

Requests made in relation to your data from a third party should be accompanied by evidence that the third party is able to act on your behalf. If this is not provided, we may contact the third party to ask that such evidence be forwarded before we comply with the request.

4. TIMESCALES

Usually, we will comply with your request without delay and at the latest within one month. Where requests are complex or numerous, we may contact you to inform you that an extension of time is required. The maximum extension period is two months.

5. FEE

We will normally comply with your request at no cost. However, if the request is manifestly unfounded or excessive, or if it is repetitive, we may contact you requesting a fee. This fee must be paid in order for us to comply with the request. The fee will be determined at the relevant time and will be set at a level which is reasonable in the circumstances.

In addition, we may also charge a reasonable fee if you request further copies of the same information.

6. INFORMATION YOU WILL RECEIVE

When you make a subject access request, you will be informed of:

a) whether or not your data is processed and the reasons for the processing of your data;
b) the categories of personal data concerning you.
c) where your data has been collected from if it was not collected from you;
d) anyone who your personal data has been disclosed to or will be disclosed to, including anyone outside of the EEA and the safeguards utilised to ensure data security;
e) how long your data is kept for (or how that period is decided);
f) your rights in relation to data rectification, erasure, restriction of and objection to processing.
g) your right to complain to the Information Commissioner if you are of the opinion that your rights have been infringed;
h) the reasoning behind any automated decisions taken about you.

7. CIRCUMSTANCES IN WHICH YOUR REQUEST MAY BE REFUSED

We may refuse to deal with your subject access request if it is manifestly unfounded or excessive, or if it is repetitive. Where it is our decision to refuse your request, we will contact you without undue

delay, and at the latest within one month of receipt, to inform you of this and to provide an explanation. You will be informed of your right to complain to the Information Commissioner and to a judicial remedy.

We may also refuse to deal with your request, or part of it, because of the types of information requested. For example, information which is subject to legal privilege or relates to management planning is not required to be disclosed. Where this is the case, we will inform you that your request cannot be complied with, and an explanation of the reason will be provided.

8. REFERENCES

The personal data included in a confidential reference is exempt from the right of access for the purpose of your prospective or actual employment. This exemption applies regardless of whether we have given or received the reference.

Despite this exemption, we will adopt a policy of openness regarding references and be as open as we can with you about personal data which relates to you.

DATA BREACH NOTIFICATION POLICY

Last Updated: June 2023

1. INTRODUCTION

We are aware of the obligations placed on us by the General Data Protection Regulation (GDPR) in relation to processing data lawfully and to ensure it is kept securely.

One such obligation is to report a breach of personal data in certain circumstances and this policy sets out our position on reporting data breaches.

2. PERSONAL DATA BREACH

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

The following are examples of data breaches:

a) access by an unauthorised third party;
b) deliberate or accidental action (or inaction) by a data controller or data processor;
c) sending personal data to an incorrect recipient;
d) computing devices containing personal data being lost or stolen;
e) alteration of personal data without permission;
f) loss of availability of personal data.

3. BREACH DETECTION MEASURES

We have implemented the following measures to assist us in detecting a personal data breach:

a) Published policies and procedures for all to report any concerns regarding their personal data
b) Regular reviews and risk assessment of the procedures and processes for collecting and storing personal data

4. INVESTIGATION INTO SUSPECTED BREACH

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by HR who will make a decision over whether the breach is required to be notified to the Information Commissioner. A decision will also be made over whether the breach is such that the individual(s) must also be notified**.**

5. WHEN A BREACH WILL BE NOTIFIED TO THE INFORMATION COMMISSIONER

In accordance with the GDPR, we will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification to the Information Commissioner will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

The following information will be provided when a breach is notified:

a) a description of the nature of the personal data breach including, where possible:

   i) the categories and approximate number of individuals concerned; and
   ii) the categories and approximate number of personal data records concerned

b) the name and contact details of HR where more information can be obtained;
c) a description of the likely consequences of the personal data breach; and
d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

6. WHEN A BREACH WILL BE NOTIFIED TO THE INDIVIDUAL

In accordance with the GDPR, we will undertake to notify the individual whose data is the subject of a breach if there is a *high* risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

The following information will be provided when a breach is notified to the affected individuals**:**

a) a description of the nature of the breach
b) the name and contact details of HR where more information can be obtained.
c) a description of the likely consequences of the personal data breach and
d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

7. RECORD OF BREACHES

The Company records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR. It records the facts relating to the breach, its effects and the remedial action taken.