



Privacy Policy

SHARPSMART.CO.UK | LAST UPDATED 3 JULY 2018

This Privacy Policy relates to the business activities of Daniels Corporation International Ltd trading as Sharpsmart Ltd ('Sharpsmart'). It applies to all suppliers of Sharpsmart in connection with the supply of products and services.



1. About this Privacy Policy

- 1.1 This Privacy Policy relates to the business activities of Daniels Corporation International Ltd trading as Sharpsmart Ltd ('Sharpsmart'). It applies to all suppliers of Sharpsmart in connection with the supply of products and services.
- 1.2 Sharpsmart may collect, use and process personal data relating to the owners, directors and staff (employees and contractors) of our customers. We do this to manage our business activities with customers and to facilitate the supply of products and services under supply contracts.
- 1.3 Sharpsmart is committed to collecting and processing personal data ('Personal Data') and sensitive personal data ('Sensitive Personal Data') in compliance with the EU General Data Protection Regulations 2018 (the 'GDPR').
- 1.4 For the purposes of this Privacy Policy, any reference to "Sharpsmart", "we", "our", or "us" means Sharpsmart Ltd as part of the global group of Daniels Health. Any reference to "you, or "your" means you as a supplier of Sharpsmart or our affiliated businesses.
- 1.5 Please read this Privacy Policy carefully as it explains how Sharpsmart collects, stores and uses your Personal Data in accordance with the GDPR.
- 1.6 We may update our Privacy Policy from time to time. Please check our website located at sharpsmart.co.uk to ensure that you are viewing the most current version of our Privacy Policy.
- 1.7 Our Data Protection Officer is Kate Chambers. You can direct any questions you may have about this Privacy Policy or about our privacy practices in general to kchambers@sharpsmart.co.uk

2. Terminology used in this Privacy Policy

"Data Access Request" is where you can ask us to provide you with a copy of the Personal Data that we hold about you (Right of Access).

"Data Breach" is a security incident where the integrity of Personal Data is compromised through being destroyed, lost, altered, corrupted, disclosed or accessed by an unauthorised person.

"Data Controller" is a legal person who controls the purposes for which and the means by which Personal Data is used.

"Data Processing" means any operation or set of operations that is performed upon Personal Data or sets of Personal Data whether automated or not including for collection, recording, organisation, structuring, storage, adaption, or alteration, retrieval, consultation, use, disclosure by transmission or for dissemination.

"Personal Data" refers to any information relating to an identifiable natural person who can be identified directly or indirectly. This includes information such as your name, email address, and contact details.

"Privacy Notice" is the document we will give you every time we collect your Personal Data, process your Personal Data for a new purpose or if we require additional Personal Data from you.

3. Data Protection Principles

3.1 As a Data Controller, we are responsible for compliance with the six GDPR principles which require that Personal Data shall:

- (a) be processed lawfully, fairly and in a transparent way;
- (b) be collected and processed only for specified, explicit and legitimate purposes;
- (c) be processed only to the extent necessary for the purposes we have notified you about;
- (d) accurate and up to date;
- (e) not be kept longer than is necessary for the purposes for which it was processed;
- (f) be processed securely.

4. The types of Personal Data we collect

4.1 We collect from our suppliers the following types of Personal Data:

- (a) business/company (name, address, email);
- (b) staff (names, job titles and department);
- (c) email address;
- (d) telephone numbers;
- (e) contract information;
- (f) payment information;
- (g) product details and service details in relation to your account;
- (h) interactions including any communications or activity;
- (i) premises security such as sign in details and CCTV footage (when on SharpSmart facilities).

5. How we collect Personal Data and our Privacy Notice

5.1 We collect and process your Personal Data when you engage with SharpSmart for business purposes. We will provide you with a Privacy Notice when you interact with us and we collect your Personal Data.

5.2 Our Privacy Notice will include the purpose of processing the Personal Data; which categories of Personal Data we will need to process; who will receive the Personal Data (including if the Personal Data needs to be shared outside of the EU); how long we will keep your Personal Data; your rights in terms of accessing your Personal Data; the consequences of failing to provide the Personal Data and details of any automated decision-making based on the Personal Data you provide.

5.3 We collect your Personal Data through a range of methods:

- (a) during the course of our business relationship;
- (b) when you contact us via telephone, email or fax;

- (c) through surveys to capture service performance and general feedback;
 - (d) update requests based on your account or the products/services we provide;
 - (e) website and online software enquiry forms;
 - (f) events and seminars;
 - (g) marketing updates either by electronic means or post.
- 5.4 We may also receive Personal Data from third parties including, for example, credit reporting agencies. If we do, we will protect your Personal Data in accordance with this Privacy Policy.

6. How we use your Personal Data

- 6.1 We collect Personal Data from our customers including owners, directors and staff for the following business purposes:
- (a) to administer and manage your business relationship with SharpSmart (for example, records establishment for contact with your staff, invoice payments, meeting our standards policies);
 - (b) to meet SharpSmart's legitimate business interests in relation to the products and services you supply to us (business administration, IT support, accounts payable, finance and data analytics);
 - (c) to meet legal, regulatory and compliance obligations.
- 6.2 If you choose to withhold your Personal Data, it may not be possible for us to interact with you for business purposes, for you to access certain parts of our website or for us to respond to your query.

7. Sharing your Personal Data with third-parties

- 7.1 We will only process and share your Personal Data with third-parties for the purposes described in this Privacy Policy.
- 7.2 We may disclose your Personal Data to any of our employees, officers, insurers, professional advisers, agents, suppliers or subcontractors insofar as reasonably necessary for the purposes set out in this Privacy Policy.
- 7.3 When we disclose your data to third parties we do so on the basis that your data is treated with confidence, and only used for the limited purpose of providing support for our business activities, and in a manner consistent with this Privacy Policy.
- 7.4 Personal Data is processed and shared with third-parties in the following ways:
- (a) third-party service providers that securely hold your data;
 - (b) to provide marketing and survey material to you (either by electronic means or post);
 - (c) third-party service providers for logistics or services;
 - (d) external HR specialists including reference and DBS related checks;
 - (e) courier service companies;
 - (f) external debt collection agencies;
 - (g) regulators and law enforcement agencies;
 - (h) with our legal representatives.

- 7.5 When we use third-parties to process your Personal Data on our behalf, we ensure that the Data Processing is pursuant to our documented instructions and in accordance with the legal basis for the processing.
- 7.6 We only employ third-party data processors that are compliant with the GDPR requirements and that have sufficient security measures in place to protect and safeguard your data.
- 7.7 If there is a change of control in our business or a sale or transfer of business assets, we reserve the right to transfer to the extent permissible at law our subscriber databases, together with any Personal Data and non-Personal Data contained in those databases.

Legal basis for collecting and processing your Personal Data

- 8.1 The legal basis for collecting and processing your Personal Data will depend on how your Personal Data is being used and how it was collected.
- 8.2 The legal basis for collecting and processing your Personal Data will be on the basis of:
 - (a) Contractual basis. This legal basis applies to the collection or processing of Personal Data in order to fulfil or perform a contract with you, or to which you are a party.
 - (b) Consensual basis. This applies where you have provided your consent to the collection or processing of Personal Data for a specific purpose (for example, to provide you with marketing updates). You can withdraw your consent at any time by updating your email preferences, opting-out, or by contacting us directly.
 - (c) Legitimate interests. This applies where we have a legitimate interest to collect or process your Personal Data. For example, it may be to respond to an enquiry about our products and services, or to improve our products and services.
 - (d) Legal obligations. This applies where it is necessary to disclose your Personal Data to comply with a legal obligation.

9. International Data Transfers

- 9.1 We may store, process and transfer your data outside of the EEA.
- 9.2 As part of our obligations under the GDPR, we only transfer the data of individuals residing in the EU to countries outside of the EU with adequate privacy data laws or to a third party where we have approved transfer mechanisms in place to protect your Personal Data (by entering into the European Commission's Standard Contractual Clauses for data protection for data that is transferred internationally or ensuring the entity is Privacy Shield certified for data transfer to third parties based in the United States).

10. How we secure your Personal Data and Data Breach

- 10.1 We are committed to ensuring that the data you provide to us is secure.
- 10.2 To prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure data and protect it from misuse, interference, loss and unauthorised access, modification and disclosure.
- 10.3 Your data will be securely stored, and all precautions will be taken to protect your data. Where possible, limitations are placed on the printing of personal data. Where this is unavoidable, data is stored in locked filing cabinets, within locked offices.

10.4 Electronic data is held as follows:

- Password protected spreadsheets
- Password protected drives
- Access controlled systems including CarrietNet and MoorePay.

10.5 We will only hold your data for as long as is necessary to fulfil the purpose for which it was collected. Periods of data retention will apply differently for each specific category of data. You will be informed of how long your data will be stored in the Privacy Notice issued to you at the time your data is collected or processed.

10.6 You can also review the Company's data register to find out more information about the data retention period for categories of data that are stored before the data is securely destroyed.

10.7 We have in place Data Breach response procedures to deal with any actual or suspected Data Breach including where we are obliged to report Data Breach to the relevant regulator within 72 hours of us becoming aware of a Data Breach. We will notify you and the applicable regulator of a Data Breach where we are legally required to do so.

10.8 You should report any actual or suspected breaches to our Data Protection Officer for investigation in the Contact us section of this policy.

11. How your Personal Data is protected

11.1 We are committed to ensuring that the Personal Data you provide to us is secure.

11.2 To prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure Personal Data and protect it from misuse, interference, loss and unauthorised access, modification and disclosure.

11.3 Your Personal Data will be securely stored, and all precautions will be taken to protect your data. Where possible, limitations are placed on the printing of personal data. Where this is unavoidable, data is stored in locked filing cabinets, within locked offices.

11.4 Personal Data that is in electronic form is held on one of the following:

- (a) password protected spreadsheets;
- (b) password protected drives; or
- (c) access controlled systems including CRM, Logistics and finance.

11.5 We will only store and process your Personal Data for as long as is necessary to fulfil the purpose for which it was collected. This will be different for various categories of data.

11.6 You will be informed of how long your Personal Data will be stored in the Privacy Notice issued to you at the time your data is collected. To find out more about how long particular categories of data are stored before the data is securely destroyed, please contact our Data Protection Officer in the Contact us section of this policy.

11.7 You can also search these records which are held in a Data Register by our external Human Resources Company; HR Experts, The Old Church, 19 Rotherham Rd, Swallownest, Sheffield S26 4UR.

12. The types of non-Personal Data we collect

- 12.1 We collect non-Personal Data from you when you visit our websites or social media pages.
- 12.2 The information collected is generally anonymous traffic data and may include your IP address, browser type, device information, and language. The information that we collect is in aggregate form so that it cannot identify any individual user.
- 12.3 We use technologies and third-party services that use Google Analytics, pixels, tags and web beacons (code snippets) on our website to improve user experience, the supply of our products and services and to analyse how our website is used.
- 12.4 We also use cookies on our website. Cookies are very small files on a website to identify visitors to our website and to store details about the use of our website. In addition, cookies may be used to serve relevant advertisements to website visitors through third party services such as Google AdWords.

13. Data Access Request (Right of Access)

- 13.1 It is important that the Personal Data we hold about you is accurate and up to date. Please keep us informed of any changes to your data.
- 13.2 We comply with your rights under the GDPR (subject to the grounds set out in the GDPR and applicable law) that permit you:
 - (a) to be informed as to how your Personal Data is being used;
 - (b) to access your Personal Data and to know specifically what information is held about you and how it is processed, where and for what purpose (we will provide you a copy of your Personal Data in electronic format free of charge if requested);
 - (c) to rectify your Personal Data if it is inaccurate or incomplete;
 - (d) to erase your Personal Data (also known as 'the right to be forgotten') if you wish to delete or remove your Personal Data;
 - (e) to restrict Data Processing of your Personal Data;
 - (f) to retain and reuse your Personal Data for your own purposes (Personal Data portability);
 - (g) to object to your Personal Data being used; and
 - (h) to object against automated decision making and profiling.
- 13.3 You can contact us any time to exercise your rights under the GDPR including as to:
 - (a) request access to Personal Data that we hold about you;
 - (b) to correct any Personal Data that we hold about you;
 - (c) delete Personal Data that we hold about you; or
 - (d) opt out of emails, marketing, and any other notifications that you receive from us.
- 13.4 We may ask you to verify your identity before acting on any of your requests. All Data Access Requests will be processed within one (1) month and will be provided in a digital format free of charge.
- 13.5 If you have any questions about the Company's collection and storage of data, please Contact us at the details set out below.

14. Staff training


14.1 We strive to create a data privacy culture within Sharpsmart and our staff regularly receive training on data protection principles and procedures both as part of the induction process and annual refresher training or as required with changes to regulations.

15. Our contact details

15.1 If you have any questions about this Privacy Policy or to submit a Data Access Request, please contact our Data Protection Officer using the details provided below.

Sharpsmart Ltd

Data Protection Officer | **Kate Chambers**

 Unit 44 Enterprise City,
Meadowfield Avenue,
Spennymoor, Co
Durham DL16 6JF

 01388 81310

 KCHAMBERS@SHARPSMART.CO.UK