Privacy, Data Protection & GDPR Policy 2018

Please Note: BDM ArcScan is a trading style of BDM Business Solutions Limited. From here on in, BDM ArcScan will be referred to as BDM Business Solutions Limited within this document.

Overview

BDM Business Solutions Limited has created the following policies to explain to our website users and visitors how we use the data collected by you visiting our website or when asked to submit any additional information regarding yourself such as in contact us forms or when you request further information.

At all times, BDM Business Solutions Limited is committed in respecting your privacy and security. We will therefore operate under the following guidelines. If you do not agree to any of the terms below, please do not submit any personal data to BDM Business Solutions Limited.

The below privacy policy is issued alongside and in guidance to our BDM Business Solutions Limited Terms and conditions.

General Data Protection Regulation, Summary

The following information is intended to summarise the main points detailing and outlining your rights as a data subject and how we (the company) handle your (the customer) data.

BDM Business Solutions Limited's full Data Protection Policy, Privacy Policy and GDPR Data Retention Policy can be viewed by reading or scrolling further down this document.

1. Your Rights as a Data Subject

The General Data Protection Regulation sets out the following rights applicable to data subjects:

a) The right to be informed;
b) The right of access;
c) The right to rectification;
d) The right to erasure (also known as the 'right to be forgotten');
e) The right to restrict processing;
f) The right to data portability;
g) The right to object;
h) Rights with respect to automated decision-making and profiling.

2. Information for Data Subjects

The following contact details are issued in the event you need to contact us regarding this policy such as for more information or if you want to act on any of the areas you are legally entitled to do so.

All such communications should be address to; **enquiries@bdmarcscan.co.uk** with a summary of how we can assist you further.

The Company's Data Protection Officer and Supervisor is Christopher Masterson. All requests are dealt with on a first come, first served bases. An acknowledgement of receipt your email will be sent back to confirm it has been received and begin our work on your request.

a) The following personal data may be collected, held, and processed by the Company for the purposes of internal record keeping and processing of customer orders:

- Customer's names and contact details.
- Card details are collected by our PCI compliant payment processing providers PayPal and World Pay and not held by the business. They are held securely by PayPal and World Pay and for the purposes only of refunds when required. The processing is necessary for the performance of a sale contract with the data subject.

b) You may request details, correction, amends, deletion, or restriction of the personal data we hold about you at any time in writing to the Company's' Data Protection Officer.

c) On occasion we will transfer your personal data to carriers, logistic providers, or other suppliers/sub-contractors for the sole purpose of fulfilment of your enquiry and /or order. Please contact our Data Protection Officer if you require specific details of any such transfer of your personal data.

d) We never transfer personal data to any third party that is located outside of the European Economic Area (the "EEA").

e) Personal data will be held by the Company for up to 6 years to meet HMRC tax obligations.

f) A data subject may withdraw their consent to the Company's processing of their personal data at any time. Please contact the Company's Data Protection Officer in writing if you wish to exercise this right. However, such action may impede future transaction with us the company.

g) A data subject may complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation) should they feel that we, we the company, have not complied fully or in part you a request made up this policy/regulation.

h) The Company does not use any automated decision-making tools or software that will use the personal data (including but not limited to profiling) provided by you.

i) We will not use your personal data for marketing purposes nor will we pass your personal data to any third party with the exception of our carriers, logistic providers or other suppliers/sub-contractors for the sole purpose of fulfilment of your order.

j) By ordering from us and therefore entering into a contract of sale with The Company, you are giving your permission for us to use and store your personal data for the purposes outlined in a) and c) above as well as detailed in full in our Data Protection Policy, Privacy Statement and
GDPR Data Retention Policy.

BDM Business Solutions Limited Privacy Policy

Background

The BDM Business Solutions Limited understands that your privacy is important to you and that you care about how your personal data is used within our company. Respecting the trust and privacy of all users visiting to our website (www.bdmarcscan.co.uk), we will only ever collect and use your personal data in the ways we will shortly describe and under our responsibilities and your rights under current binding law and regulation.

We recommend users intending to use our website for any purposes carefully read the following information and understand is content and implications fully.

By entering our website (to view, download, enquire or complete a sale), it is deemed you have read and understand our privacy policy fully and accept it fully. If however, you do not accept and agree to our privacy policy in full or in part, you must stop using our website immediately and stop any activity such as submitting an enquiry or completing a sale through our ecommerce platform.

If in any doubt, please contact us as detailed previously.

1. Definitions and Interpretation
In this Policy, the following terms shall have the following meaning/s:

"**Account**" means an account required to access and/or use certain areas and features of our website;

"**Cookie**" means a small text file placed on your computer or device by our website when you visit certain parts of our website and/or when you use certain features of our website. Details of the Cookies used by our website are set out in section 13, below;

"**Cookie Law**" means the relevant parts of the Privacy and Electronic Communications (EC Directive) Regulations 2003;

"**personal data**" means any and all data that relates to an identifiable person who can be directly or indirectly identified from that data. In this case, it means personal data that you give to us via our website.

This definition shall, where applicable, incorporate the definitions provided in the Data Protection Act 1998 OR EU Regulation 2016/679 – the General Data Protection Regulation ("GDPR"); and

"**We/Us/Our**" means BDM Business Solutions Limited, a limited company registered in England under company number 05024385, whose registered address is 1 Darin Court, Crownhill, Milton Keynes, MK8 0AD, UK.

2. Information About Us
2.1 Our website is owned, operated, and maintained by BDM Business Solutions Limited, a limited company registered in England under company number 05024385, whose registered address is 1 Darin Court, Crownhill, Milton Keynes, MK8 0AD, UK.

2.2 Our VAT number is GB 824 9390 08

2.3 Our Data Protection Officer is Christopher Masterson who can be contacted by via email using the following address; enquiries@bdmarcscan.co.uk.

3. What Does This Policy Cover?
This Privacy Policy only applies to the use of our website, www.bdmarcscan.co.uk.

Our website may contain links to other websites to aid your user experience, finding out additional information or completing your sale for example. In the event such action is required, you will be notified that you will be leaving our website and linked to another website.

BDM Business Solutions Limited do not have any control over such external links and sources in the way they may obtain, collate, store, or use your personal data and information. We advise that on first entering any enteral link/source, you read their privacy policy or polices to make an informed decision on how their processes work and before continuing to use their service/s or provide any personal data and information.

4. Your Rights

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

4.1.1 The right to be informed about how and why we collect and use your personal data;
4.1.2 The right of access to the personal data we hold about you (see section 12);
4.1.3 The right to rectification if any personal data we hold about you is inaccurate, misleading, or incomplete (please contact us using the details in section 14);
4.1.4 The right to be forgotten – e.g. the right to ask us to delete any personal data we hold about you (we only hold your personal data for a limited time, as explained in section 6 but if you would like us to delete it sooner, please contact us using the details in section 14);
4.1.5 The right to restrict (i.e. prevent) the processing of your personal data;
4.1.6 The right to data portability (obtaining a copy of your personal data to re-use with another service or organisation);
4.1.7 The right to object to Us using your personal data for particular purposes; and
4.1.8 Rights with respect to automated decision making and profiling.

4.2 If you have any cause for complaint about our use of your personal data, please contact us using the details provided in section 14 and we will do our best to resolve any problem/s for you. If we are unable to help, you also have the right to make a complaint to 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 seek approved and professional third-party advice.

5. What Data Do We Collect?

Depending on how you use our website, we may collect some or all of the following personal [and non-personal] data (please also see section 13 on Our use of Cookies and similar technologies)

5.1 Name (in full including title);
5.2 Business/company name
5.3 Job title/position;
5.4 Profession/occupation;
5.5 Contact information such as email addresses, postal address, and telephone numbers;
5.6 Demographic information such as post code;
5.7 Financial information such as credit / debit card numbers;
5.8 IP address;
5.9 Web browser type and version;
5.10 Operating system;
5.11 a list of URLs starting with a referring site, your activity on our website, and the website you exit/leave to;

6. How Do We Use Your Data?

6.1 All personal data received via our website 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 Data Protection Act 1998 and/or GDPR at all times. For more details on security see section 7, below.

6.2 Our use of your personal data will always have a lawful basis, either because it is necessary for us to perform an action you have requested such as sale/contract, because you have agreed to our use of your personal data such as subscribing to an email newsletter/promotion or it is because it is within our legitimate and genuine interests. Specifically, we will or may use your data for the following purposes:

6.2.1 Providing and managing your Account;
6.2.2 Providing and managing your access to our website;

6.2.3 Personalising and tailoring your experience on our website;
6.2.4 Supplying our products AND/OR services to you (please note that we require your personal data in order to enter into a contract with you);
6.2.5 Personalising and tailoring our products AND/OR services for you;
6.2.6 Replying to emails from you;
6.2.7 Market research;
6.2.8 Analysing your use of our website and gathering feedback to enable us to continually improve our website and your user experience;

6.3 With your permission and/or where permitted by law, we may also use your data for marketing purposes which may include contacting you by email with information, news and offers on our products AND/OR services. We will not, however, send you any unsolicited marketing or spam and will take all practical steps to ensure that we fully protect your rights and comply with our obligations under the Data Protection Act 1998 and/or GDPR and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

6.4 You have the right to withdraw your permission allowing us to use your personal data at any time, and to request that we completely delete it or provide a copy of the information we have.

6.5 We do not keep your personal data for any longer than is necessary in light of the reason(s) for which it was first collected or requested. Data will therefore be retained for the following periods (or its retention will be determined on the following bases):
6.5.1 6 years maximum from last recorded contact with you
After this period, your data will be securely and confidentially destroyed.

7. How and Where Do We Store Your Data?
7.1 We only keep your personal data for as long as We need to in order to use it as described above in section 6, and/or for as long as We have your permission to keep it.

7.2 Your data will only be stored within the UK or the European Economic Area ("the EEA") (The EEA consists of all EU member states, plus Norway, Iceland, Liechtenstein).

7.3 Data security is extremely important to us and we have taken and will continue to take all necessary measures to safeguard and secure your personal information entered via our website and also for its permitted storage on our servers when received from our website.

8. Do We Share Your Data?

8.1 We may share your data with other companies in our group because it is necessary to perform an action as part of your interaction with us such as providing more information, completing a sale, or providing a service. This also includes our subsidiaries.

8.2 We may sometimes engage with third parties to supply products and services to you on our behalf to complete our contract and obligations to you. These may include but not limited to payment processing, delivery of goods, search engine facilities, maintenance, after sales care, advertising, and marketing. Such third parties may require access to some or all of your data provided to us. We will endeavour to take reasonable steps and precautions to ensure your data is handled safely, securely and in accordance your rights, our obligations, and the obligations of the third party under the law.

8.3 We may compile and collate statistics about how users interact with our website 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 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.

8.4 We may sometimes use third party data processors that are located outside of the UK or the European Economic Area ("the EEA") (The EEA consists of all EU member states, plus Norway, Iceland, and Liechtenstein). Where We transfer any personal data outside the EEA, we will take all

reasonable steps and endeavours to ensure that your data is treated as safely and securely as it would be within the UK and under the Data Protection Act 1998 and/or GDPR.

8.5 In certain circumstances and conditions, 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.

9. What Happens If Our Business Changes Hands?
9.1 We may, from time to time, expand or reduce our business operations and this may involve the sale and/or the transfer of control of all or part of our business. 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.

9.2 In the event that any of your data is to be transferred in such a manner, you will not be contacted in advance and informed of the changes.

10. How Can You Control Your Data?
10.1 In addition to your rights under the GDPR, set out in section 4, when you submit personal data via our website, you may be given options to restrict our use of your data. In particular, we aim to give you a clean and understandable explanation of how we would like to use your submitted data such as for direct marketing purposes. You can choose to opt out of receiving any such communications by, for example, using an unsubscribe feature, emailing the sender back or confirm your communication preferences with your account manager. Such changes can take up to 7 to 10 days to be truly effective and we apologise for any additional communications sent within this period as your preferences are updated throughout the business.

10.2 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 stop and prevent you receiving unsolicited marketing materials by telephone and/or email. Please note, however, that these services will not prevent you from receiving marketing communications and materials that you have consented to receiving and these services may require you to update your preferences with them on annual basis. It is your responsibility to provide such service providers with updated information as and when it becomes relevant. Please check their terms and conditions for additional advice and support on how these services work and operate.

11. Your Right to Withhold Information
11.1 You may access certain areas of our website without providing any data at all. However, to use all features and functions available on our website, you may be required to submit or allow for the collection of certain data.

11.2 You may restrict Our use of Cookies.

12. How Can You Access Your Data?
You have the right to ask for a copy of any of your personal data held by us (where such data is held). Under the GDPR, no fee is payable, and we will provide any and all information in response to your request free of charge and within a reasonable period.

Please contact Us for more details at enquiries@bdmarcscan.co.uk, or using the contact details below in section 14.

13. Our Use of Cookies
"Cookies" are small pieces of information that are issued to your computer when you enter a website (such as ours, www.bdmarcscan.co.uk). Cookies are stored by your browser on your computer's hard drive, and they can be used for a wide range of purposes, such as identifying your computer's previous visits to the Website, and to ascertain the most popular features of the Website accessed or interacted with.

13.1 Our website 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 of our website and to provide and improve our products AND/OR services. Such cookies have been carefully chosen, tested, and monitored to ensure they operate correctly and are securely handling your privacy and personal data.

13.2 All Cookies used by and on our website are used in accordance with current Cookie Law.

13.3 Before Cookies are placed on your computer or device, you will be shown a prompt requesting your consent to set those Cookies and an option to find out more which will revert you to this document and the areas which relate to Cookies. The prompt will remain visible until you have acknowledged the message. By clicking OK or Yes, you are consenting to us placing Cookies on your equipment and agree to their usage rights as detailed in this document. You can also choose to deny placing Cookies on your equipment by clicking No or Cancel. However, your user experience of our website maybe more limited and not function as intended.

13.4 Certain features of our website depend on Cookies to function correctly or at their optimum. Cookie Law considers these Cookies to be “strictly necessary”. These Cookies are shown below in section 13.6. Your consent will not be sought to place these Cookies on the computer or device you are using to access our website, but it is still important that you are aware of their existence and why they are needed. You do however have the option to block these Cookies by changing the configuration of your chosen internet browser, detailed in section 13.10. However, your user experience of our website maybe more limited and not function as intended.

13.5 Our website uses analytics services provided by Google and Bing (Microsoft). Website analytics refers to a set of tools used to collect and analyse anonymous usage information, allowing us to better understand how our website is used. This can then allow us to continually look at improving how our website works and the products and/or services we offer though this medium. While you do not need to allow us to use these Cookies for the purposes stated before, they do enable a better user experience for you and, as stated, are fully secure, verified and monitored to ensure they pose no risk to your privacy and safety.

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

13.7 In addition to the controls that we provide in controlling Cookies, you can also choose to enable or disable Cookies in your internet browser via their configurable settings. While setting controls will vary between different internet browser providers, most will allow you to choose to disable all cookies or only third-party cookies. The default setting for many will be to accept cookies. For more information and guidance, please consult your internet browser’s user guide or support services. Please note, the settings you apply will affect your web browser as a whole and not just for our website.

13.8 You can choose to delete Cookies on your computer or device at any time using your web browser’s settings or by some internet security programmes. Please note that such action will cause you to lose information that may help you access and use our website more quickly and easily including, but not limited to login and personalisation settings.

13.9 You are responsible for ensuring that the computer or device you are using to access our website has the latest up to date version of both your preferred internet browser and operating system. You should also consult either about how to adjust your privacy settings if you are in any doubt and making such changes.

14. Contacting Us

If you have any questions about our website or this Privacy Policy, please contact us by email at enquiries@bdmarcscan.co.uk. Please include a summary of your request particularly if it is a request for information about the data We hold about you (as under section 12, above).

15. Changes to Our Privacy Policy
We will review this Privacy Policy on an annual basis to make any changes or sooner if there is a change in law which we must abide or include. Such changes will be immediate and will replace any presently active and viewable Privacy Policy. You will have been deemed to have accepted any revised Privacy Policy on your first use of our website following any such change/s.

You are advised to check the Privacy Policy page on a regular basis for any updates and amendments.

1. Introduction
This Data Protection Policy sets out the obligations of BDM Business Solutions Limited ("the Company") regarding data protection and the rights of customers, business contacts, etc. ("data subjects") in respect of their personal data under the General Data Protection Regulation, also known as GDPR ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Data Protection Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles
This Policy aims to ensure compliance with the Regulation. The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be:

a) Processed lawfully, fairly, and in a clear manner in relation to the data subject;
b) Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is unsuited with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased, or rectified without delay;
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject;
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. Lawful, Fair, and Transparent Data Processing
The Regulation seeks to ensure that personal data is processed lawfully, fairly, and clearly, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be legitimate if at least one of the following applies:

a) the data subject has given permission to the processing of his or her personal data for one or more specific purposes;
b) processing is required for the purposes of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is required for compliance with a legal obligation to which the controller is subject;
d) processing is required to protect the important interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental

rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. Processed for Specified, Explicit and Legitimate Purposes

4.1 The Company collects and processes the personal data set out in Part 21 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us).

4.2 The Company only processes personal data for the exact purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the Regulation). The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected, where it is collected directly from them, or as soon as possible (not more than one calendar month) after collection where it is obtained from a third party.

5. Adequate, Relevant and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. Accuracy of Data and Keeping Data Up To Date

The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at 6-yearly intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate. Data will only be held for up to 6-years to comply with the Company's HMRC obligations.

7. Timely Processing

The Company shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay in a secure, confidential method.

8. Secure Processing

The Company shall confirm that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing, access and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Data Protection Policy.

9. Accountability

9.1 The Company's data protection officer is Christopher Masterson

9.2 The Company shall keep written and/or virtual internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) The name and details of the Company, its data protection officer, and any applicable third-party data controllers;

b) The purposes for which the Company processes personal data;

c) Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates;

d) Details (and categories) of any third parties that will receive personal data from the Company;

e) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;

f) Details of how long personal data will be retained by the Company; and

g) Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

10. Privacy Impact Assessments

The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Company's data protection officer and shall address the following areas of importance:

10.1 The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data;

10.2 Details of the legitimate interests being pursued by the Company;

10.3 An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
10.4 An assessment of the risks posed to individual data subjects; and
10.5 Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation.

11. The Rights of Data Subjects

The Regulation sets out the following rights applicable to data subjects:

a) The right to be informed;
b) The right of access;
c) The right to rectification;
d) The right to erasure (also known as the 'right to be forgotten');
e) The right to restrict processing;
f) The right to data portability;
g) The right to object;
h) Rights with respect to automated decision-making and profiling.

12. Keeping Data Subjects Informed

12.1 The Company shall ensure that the following information is provided to every data subject when personal data is collected:

a) Details of the Company including, but not limited to, the identity of Christopher Masterson, its Data Protection Officer;
b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;
c) Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
e) Where the personal data is to be transferred to one or more third parties, details of those parties;
f) Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 24 of this Policy for further details concerning such third country data transfers);
g) Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);
h) Details of the data subject's rights under the Regulation;
i) Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;
j) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);
k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;
l) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

12.2 The information set out above in Part 12.1 shall be provided to the data subject at the following applicable time:
12.2.1 Where the personal data is obtained from the data subject directly, at the time of collection;
12.2.2 Where the personal data is not obtained from the data subject directly (i.e. from another party):

a) If the personal data is used to communicate with the data subject, at the time of the first communication; or

b) If the personal data is to be disclosed to another party, before the personal data is disclosed; or
c) In any event, not more than one month after the time at which the Company obtains the personal data.

13. Data Subject Access

13.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).
13.2 All subject access requests received must be forwarded to Christopher Masterson, the Company's data protection officer by email, **enquiries@bdm-technology.com**
13.3 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.
13.4 The Company reserves the right to request initial details from yourself to ensure the person requesting such information is genuine. This may require proof of ID or interaction with the Company on a previous occasion.

14. Rectification of Personal Data

14.1 If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).
14.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data.

15. Erasure of Personal Data

15.1 Data subjects may request that the Company erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;
b) The data subject wishes to withdraw their consent to the Company holding and processing their personal data;
c) The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object);
d) The personal data has been processed unlawfully;
e) The personal data needs to be erased in order for the Company to comply with a particular legal obligation [;] OR [.]
f) [The personal data is being held and processed for the purpose of providing information society services to a child.]

15.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension).
15.3 In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

16.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

17. Data Portability

17.1 The Company processes personal data using automated means: via ecommerce and 3rd party marketplace ordering/checkout website pages.

17.2 Where data subjects have given their consent to the Company to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

17.3 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format[s]:

a) Microsoft Excel spreadsheet.

17.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to another data controller.

17.5 All requests for copies of personal data shall be complied with within one month of the data subject's request (this can be extended by up to two months in the case of complex requests in the case of complex or numerous requests, and in such cases the data subject shall be informed of the need for the extension).

18. Objections to Personal Data Processing

18.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), [and processing for scientific and/or historical research and statistics purposes].

18.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms; or the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.

18.4 Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. Automated Decision-Making

19.1 In the event that the Company uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company.

19.2 The right described in Part 19.1 does not apply in the following circumstances:

a) The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject;

b) The decision is authorised by law; or

c) The data subject has given their explicit consent.

20. Profiling

Where the Company uses personal data for profiling purposes, the following shall apply:

a) Clear information explaining the profiling will be provided, including its significance and the likely consequences;

b) Appropriate mathematical or statistical procedures will be used;

c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and

d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

21. Personal Data

The following personal data may be collected, held, and processed by the Company:

a) internal record keeping/processing of customer orders: customer's names and contact details. Card details are collected for payment by World Pay and/or PayPal and not held by the business. They are held securely by World Pay and PayPal and for the purposes only of refunds when required or repeat transactions when the customer requests. The processing is necessary for the performance of a sale contract with the data subject.

22. Data Protection Measures

The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a) All emails containing personal data must be encrypted using TLS;
b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely using built-in software deletion processes.
c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email, and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
f) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
g) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Royal Mail Special Delivery;
h) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from Christopher Masterson.
i) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;
j) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of Christopher Masterson;
k) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;
l) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
m) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise [without the formal written approval of Christopher Masterson], and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary].
n) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the

Regulation (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);
o) All personal data stored electronically should be backed up daily with backups stored offsite.
p) All electronic copies of personal data should be stored securely using passwords;
q) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols [. All software used by the Company is designed to require such passwords];
r) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.
s) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Christopher Masterson to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least yearly.

23. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a) All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;
b) Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
c) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
d) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
e) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
f) The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
g) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;
h) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation;
i) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

24. Transferring Personal Data to a Country Outside the EEA

24.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.
24.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
c) The transfer is made with the informed consent of the relevant data subject(s);
d) The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
e) The transfer is necessary for important public interest reasons;
f) The transfer is necessary for the conduct of legal claims;
g) The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

25. Data Breach Notification

25.1 All personal data breaches must be reported immediately to the Company's data protection officer.
25.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
25.3 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 25.2) to the rights and freedoms of data subjects, the data protection officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
25.4 Data breach notifications shall include the following information:

a) The categories and approximate number of data subjects concerned;
b) The categories and approximate number of personal data records concerned;
c) The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained);
d) The likely consequences of the breach;
e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

26. Implementation of Policy

This Policy shall be deemed effective as of Thursday 25th June 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

BDM Business Solutions Data Retention Policy

1. Introduction

This Data Retention Policy sets out the responsibilities of BDM Business Solutions Limited, a limited company registered in England under company number 05024385, whose registered address is 1 Darin Court, Crownhill, Milton Keynes, MK8 0AD, UK ("the Company") regarding the retaining of personal data collected, held, and processed by the Company in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

The GDPR defines "personal data" as any information relating to an identified or identifiable natural person (a "data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
b) When the data subject withdraws their consent;
c) When the data subject objects to the processing of their personal data and the Company has no overriding legitimate interest;
d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);
e) When the personal data has to be erased to comply with a legal obligation; or
f) Where the personal data is processed for the provision of information society services to a child.

This Policy sets out the type(s) of personal data held by the Company [for the performance of a sale contract with the data subject.], the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

For further information on other aspects of data protection and compliance with the GDPR, please refer to the Company's Data Protection Policy.

2. Aims and Objectives

2.1 The primary aim of this Policy is to set out limits for the holding of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to safeguard that the Company complies fully with its responsibilities and the rights of data subjects under the GDPR.

2.2 In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that unnecessary amounts of data are not retained by the Company, this Policy also aims to improve the speed and effectiveness of managing data.

3. Scope

3.1 This Policy applies to all personal data held by BDM Business Solutions Limited AND/OR for the performance of a sale contract with the data subject. [and by third-party data processors processing personal data on the Company's behalf].

3.2 Personal data, as held by the Company OR the above is stored in the following methods and locations:

a) The Company's main server located in Milton Keynes;
b) Third-party servers operated World Pay and located in the United Kingdom; PayPal and located in the United Kingdom;
c) Computers permanently located in the Company's premises at Milton Keynes, Manchester, and Cheshire
d) Physical records stored in Milton Keynes.

4. Data Subject Rights and Data Integrity

All personal data held by the Company is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Company's Data Protection Policy.

4.1 Data subjects are kept fully up-to-date of their rights, of what personal data the Company holds about them, how that personal data is used [as set out in Parts 12 and 13 of the Company's Data Protection Policy], and how long the Company will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).

4.2 Data subjects are given control over their personal data held by the Company including the right to have incorrect data corrected, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Company's use of their personal data, [the right to data portability,] and further rights relating to automated decision-making and profiling [, as set out in Parts 14 to 20 of the Company's Data Protection Policy].

5. Technical and Organisational Data Security Measures

5.1 The following practical measures are in place within the Company to protect the security of personal data. Please refer to Parts 22 to 26 of the Company's Data Protection Policy for further details:

a) All emails containing personal data must be encrypted;
b) All emails containing personal data must be marked "confidential";
c) Personal data may only be transmitted over secure networks;
d) Personal data must be transmitted over only secure wireless or wired network;
e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email, and stored securely. The email itself and associated temporary files should be deleted;
f) Where personal data is to be sent by facsimile transmission (fax) the recipient should be informed in advance and should be waiting to receive it;
g) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient or sent using an approved delivery source;
h) All personal data transferred physically should be transferred in a suitable container marked "confidential";
i) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from Christopher Masterson, Data Protection Officer.
j) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;
k) No personal data may be moved to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without authorisation;
l) Personal data must be handled with care at all times and should not be left unattended or on view;
m) Computers used to view personal data must always be locked before being left unattended;
n) No personal data should be stored on any mobile device, whether such device belongs to the Company or otherwise [without the formal written approval of the Data Protection Officer and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary];
o) [No personal data should be transferred to any device personally belonging to an employee and personal. Data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in

question has agreed to comply fully with the Company's Data Protection Policy and the GDPR;]

p) All personal data stored electronically should be backed up daily or more frequently with backups stored onsite AND/OR offsite. All backups should be encrypted;

q) All electronic copies of personal data should be stored securely using passwords and encryption;

r) All passwords used to protect personal data should be altered regularly and should must be secure;

s) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method.

t) All software should be kept up-to-date. Security-related updates should be installed not more than 2 months OR as soon as reasonably possible after becoming available;

u) No software may be installed on any Company-owned computer or device without approval; and

v) Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the Data Protection Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

5.2 The following organisational measures are in place within the Company to protect the security of personal data. Please refer to Part 27 of the Company's Data Protection Policy for further details:

a) All employees and other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under the Company's Data Protection Policy;

b) Only employees and other parties working on behalf of the Company that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Company;

c) All employees and other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

d) All employees and other parties working on behalf of the Company handling personal data will be appropriately supervised;

e) All employees and other parties working on behalf of the Company handling personal data should exercise care and caution when discussing any work relating to personal data at all times;

f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

g) The performance of those employees and other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

h) All employees and other parties working on behalf of the Company handling personal data will be bound by contract to comply with the GDPR and the Company's Data Protection Policy;

i) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Company arising out of the GDPR and the Company's Data Protection Policy;

j) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under the GDPR and/or the Company's Data Protection Policy, that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

6.1 Personal data stored electronically (including any and all backups thereof) shall be deleted [securely using the data delete method];
6.2 Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely using the: not applicable – no special category personal data held - method;
6.3 Personal data stored in hardcopy form shall be shredded [to at least P-4] and recycled
6.4 Special category personal data stored in hardcopy form shall be shredded to at least: not applicable – no special category personal data held.

7. Data Retention

7.1 As stated above, and as required by law, the Company shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.
7.2 Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.
7.3 When establishing and/or reviewing retention periods, the following shall be taken into account:

a) The objectives and requirements of the Company;
b) The type of personal data in question;
c) The purpose(s) for which the data in question is collected, held, and processed;
d) The Company's legal basis for collecting, holding, and processing that data;
e) The category or categories of data subject to whom the data relates;
f) HMRC tax obligations.

7.4 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.
7.5 Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Company to do so (whether in response to a request by a data subject or otherwise).
7.6 [In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be

8. Roles and Responsibilities

8.1 The Company's Data Protection Officer is Christopher Masterson
8.2 The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.
8.3 The Data Protection Officer shall be directly responsible for ensuring compliance with the above data retention periods [throughout the Company].
8.4 Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

9. Implementation of Policy

This Policy shall be deemed effective as of 1.4.18. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Privacy, Data Protection & GDPR Policy has been approved and authorised by:

Name: Martyn Price
Position: Director
Date: Thursday 25th May 2018
Due for Review by: Friday 24th May 2019

Signature;

Name: Christopher Masterson
Position: Data Protection Officer
Issue Date: Thursday 25th May 2018
Due for Review by: Friday 24th May 2019

Signature;