# Just Care Products Ltd GDPR Compliance Statement

## Introduction

The ***EU General Data Protection Regulation ("GDPR")*** came into force across the European Union on 25th May 2018 and brought with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

## Our Commitment

**Just Care Products Ltd** are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. We recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the Isle of Man Data Protection Act 2018

**Just Care Products Ltd** are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

## How We Have Prepared for the GDPR

- ***Data Protection*** – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.
- ***Data Retention & Erasure*** – we have updated our retention policy and schedule to ensure that we meet the *'data minimisation'* and *'storage limitation'* principles and that personal information is stored and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new *'Right to Erasure'* obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
- ***Data Breaches*** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
- ***International Data Transfers & Third-Party Disclosures*** – Not applicable as the only

personal information we will hold will be for VAT purposes within the Isle of Man, or to enable the company to deliver products to our customer.

  - ***Subject Access Request (SAR)*** – we have SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

- ***Legal Basis for Processing*** - we have reviewed processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- ***Privacy Notice/Policy*** – we have renewed our Privacy Notice to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- ***Obtaining Consent*** – we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with date records; and an easy to see and access way to withdraw consent at any time, where legal (VAT Relief forms are withdrawn and securely destroyed once the 7 Year time allowable is reached).
- ***Direct Marketing*** – we have revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials. (Just Care Products do not do direct marketing at present, but have left this wording in for legal reasons).
- ***Data Protection Impact Assessments (DPIA)*** – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s). (Just Care Products store VAT forms in a locked filing cabinet; is never shared with 3rd Parties and is destroyed after the 7 year time limit has been reached).
- ***Processor Agreements*** – where we use any third-party to process personal information on our behalf (*i.e. Payroll, Recruitment, Hosting etc*), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (*as well as we*), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.
- ***Special Categories Data*** **-** where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit

and is verified by a signature, with the right to modify or remove consent being clearly signposted. (Not applicable to Just Care Products)

## Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via our website and instore, of an individual's right to access any personal information that **Just Care Products Ltd** processes about them and to request information about: -

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

## Information Security & Technical and Organisational Measures

**Just Care Products Ltd** takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including

: no personal information is kept on the computer without password protection (in our old invoicing system (pre Sept 2017)
: any names and addresses on our current accounting system (Xero) is encrypted and password protected.
: any forms for VAT purposes are kept in a locked filing cabinet

## GDPR Roles and Employees

**Just Care Products Ltd** have designated **Amy Maguire (Director)** as our **GDPR Appointed Person.**

**Just Care Products Ltd** understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR