

**DATA PROTECTION POLICY**

**To the requirements of the**

**General Data Protection Regulation [GDPR]**

 **(EU) 2016/679**

GDPR\_DOC\_1.3

|  |  |  |  |
| --- | --- | --- | --- |
| Issue Date: | 22/02/2022 | Copy No. | 1 (Master) |
| Authorised By: | Stephen Manley | Holder: | Stephen Manley |
| Signature: |  | Signature: |  |

**Circulation List**

This policy is a controlled document and is maintained on the server as read only. The Data Protection Officer must ensure that all amendments are circulated and obsolete copies removed and filed. Hard copies used for training and internal auditing are controlled and distributed as follows.

**Copy No. Holder**

1 Data Protection Officer

**Amendment History**

This **policy** is reviewed periodically, at least annually, and is retained for a period of 5 years. Amendments and revisions are distributed to the named holders. The history of amendments and the issue of revisions are recorded below.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date** | **Amend. No.** | **Page No.** | **New Issue No.** | **Reason for Change** | **Authorised By** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 22/02/2022 | 2 | ALL | 3 | Change of Aim and Scope of policy, Add Data Security, add Breach Notification | Stephen Manley |
|  | 3 |  | 4 |  |  |
|  | 4 |  | 5 |  |  |
|  | 5 |  | 6 |  |  |
|  | 6 |  | 7 |  |  |
|  | 7 |  | 8 |  |  |
|  | 8 |  | 9 |  |  |
|  | 9 |  | 10 |  |  |
|  | 10 |  | 11 |  |  |
|  | 11 |  | 12 |  |  |
|  | 12 |  | 13 |  |  |
|  | 13 |  | 14 |  |  |
|  | 14 |  | 15 |  |  |
|  | 15 |  | 16 |  |  |
|  | 16 |  | 17 |  |  |

Copies of this document other than those listed above will not be revised; such copies will be marked as **UNCONTROLLED**.

**Table of Contents**

Contents

[1. Context and Overview 4](#_Toc516583344)

[Introduction 4](#_Toc516583345)

[Aim and Scope of Policy 4](#_Toc516583346)

[2. People, risks and responsibilities 5](#_Toc516583347)

[Data protection risks 5](#_Toc516583349)

[Responsibilities 5](#_Toc516583350)

[General staff guidelines 7](#_Toc516583351)

[3. Data SECURITY 7](#_Toc516583352)

[Data storage 8](#_Toc516583353)

[Data use 9](#_Toc516583353)

[Data accuracy 9](#_Toc516583354)

[5. Breach notification 10](#_Toc516583355)

[6. Subject access requests 10](#_Toc516583355)

[Disclosing data for other reasons 10](#_Toc516583356)

[Providing information 11](#_Toc516583357)

**DATA PROTECTION POLICY**

# Context and Overview

**Key Details**

* Policy Prepared By: Stephen Manley
* Approved by Board/Management On: 22/02/2022
* Policy Effective Date: 22/02/2022
* Reviewed by Stephen Manley on 22/02/2022
* Next Review Date: 22/02/2023

**Introduction**

RUMMAN CARE LTDneeds to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company’s data protection standards — and to comply with the law.

1. **Aim and scope of policy**

This policy applies to the processing of personal data in manual and electronic records kept by Rumman Care Ltd in connection with its human resources function as described below. It also covers Rumman Care Ltd response to any data breach and other rights under the General Data Protection Regulation and current Data Protection Act.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

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

“Special categories of personal data” is data which relates to an individual’s health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

“Criminal offence data” is data which relates to an individual’s criminal convictions and offences.

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

Rumman Care Ltd makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of Rumman Care Ltdthe Company will ensure that the third party takes such measures in order to maintain the Company’s commitment to protecting data. In line with current data protection legislation, Rumman Care Ltd understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

This policy applies to:

* The head office of RUMMAN CARE LTD
* All branches of RUMMAN CARE LTD
* All staff and volunteers of RUMMAN CARE LTD
* All Rumman Care Ltd Clients or Service Users
* All contractors, suppliers and other people working on behalf of RUMMAN CARE LTD

Types of data held

Personal data is kept in personnel files or within the Company’s HR systems. The following types of data may be held by the Company, as appropriate, on relevant individuals:

* name, address, phone numbers - for individual and next of kin
* CVs and other information gathered during recruitment
* references from former employers
* National Insurance numbers
* job title, job descriptions and pay grades
* conduct issues such as letters of concern, disciplinary proceedings
* holiday records
* internal performance information
* medical or health information
* sickness absence records
* tax codes
* terms and conditions of employment
* training details.

Relevant individuals should refer to Rumman Care Ltd privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

1. **People, risks and responsibilities**

**Data protection risks**

This policy helps to protect RUMMAN CARE LTD from some very real data security risks, including:

* Breaches of confidentiality. For instance, information being given out inappropriately.
* Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
* Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

**Responsibilities**

Everyone who works for or with RUMMAN CARE LTD has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The board of directors is ultimately responsible for ensuring that RUMMAN CARE LTD meets its legal obligations.

The data protection officer, Stephen Manley, is responsible for:

* Keeping the board updated about data protection responsibilities, risks and issues.
* Reviewing all data protection procedures and related policies, in line with an agreed schedule.
* Arranging data protection training and advice for the people covered by this policy.
* Handling data protection questions from staff and anyone else covered by this policy.
* Dealing with requests from individuals to see the data RUMMAN CARE LTD holds about them (also called ‘subject access requests’).
* Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.

The IT manager, is responsible for:

* Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
* Performing regular checks and scans to ensure security hardware and software is functioning properly.
* Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

The Directors, Stephen Manley & Kevin Rummun, are responsible for:

* Approving any data protection statements attached to communications such as emails and letters.
* Addressing any data protection queries from journalists or media outlets like newspapers.
* Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

**General staff guidelines**

* The only people able to access data covered by this policy should be those who need it for their work.
* Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
* RUMMAN CARE LTD will provide training to all employees to help them understand their responsibilities when handling data.
* Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
* In particular, strong passwords must be used, and they should never be shared.
* All correspondence in regard to young people, must have a pseudo name (refer to anonymisation of data policy).
* Personal data should not be disclosed to unauthorised people, either within the company or externally.
* Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
* Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.
1. **Data security**

Rumman Care Ltd. adopts procedures designed to maintain the security of data when it is stored and transported. More information can be found in the data transfer security policy, available from theData Protection Officer.

In addition, employees must:

* Ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
* Ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
* Refrain from sending emails containing sensitive work-related information to their personal email address
* Check regularly on the accuracy of data being entered into computers
* Always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
* Use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by *The Data Protection Officer or the CEO.* Where personal data is recorded on any such device it should be protected by:

* Ensuring that data is recorded on such devices only where absolutely necessary
* Using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
* Ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow Rumman Care Ltd. rules on data security may be dealt with via Rumman Care Ltd. disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

**Data storage**

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data protection officer.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

* When not required, the paper or files should be kept in a locked drawer or filing cabinet.
* Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
* Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access,

accidental deletion and malicious hacking attempts:

Data should be protected by strong passwords that are changed regularly and never shared between employees.

* Data should not be stored on a removable device, such as a USB stick or CD.
* Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
* Servers containing personal data should be sited in a secure location, away from general office space.
* Data should be backed up frequently. Those backups should be tested regularly, in line with the company’s standard backup procedures.
* Data should never be saved or stored directly on personal devices or to laptops or other mobile devices like tablets or smart phones.
* All servers and computers containing data should be protected by approved security software and a firewall.

**Data use**

Personal data is of no value to RUMMAN CARE LTD unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

* When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
* Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
* Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
* Personal data should never be transferred outside of the European Economic Area.
* Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

**Data accuracy**

The law requires RUMMAN CARE LTD to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort RUMMAN CARE LTD should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

* Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
* Staff should take every opportunity to ensure data is updated. For instance, by confirming a young person’s details when they arrive.
* RUMMAN CARE LTD will make it easy for data subjects to update the information RUMMAN CARE LTD holds about them. For instance, via the company website.
* Data should be updated as inaccuracies are discovered. For instance, if a social worker can no longer be reached on their stored telephone number/email address, it should be removed from the database.
* It is the marketing manager’s responsibility to ensure marketing databases are checked against industry suppression files every six months.
1. **Breach notification**

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner (ICO) within 72 hours of Netpex becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, Netpex will do so without undue delay.

1. **Subject access requests**

All individuals who are the subject of personal data held by RUMMAN CARE LTD are entitled to:

* Ask what information the company holds about them and why.
* Ask how to gain access to it.
* Be informed how to keep it up to date.
* Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data protection officer at info@rummancare.co.uk

. The data protection officer can supply a standard request form, although individuals do not have to use this.

Individuals will be charged £10 per subject access request. The data protection officer will aim to provide the relevant data within 14 days. The data protection officer will always verify the identity of anyone making a subject access request before handing over any information.

**Disclosing data for other reasons**

In certain circumstances, the General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, RUMMAN CARE LTD will disclose requested data. However, the data protection officer will ensure the request is legitimate, seeking assistance from the board and from the company’s legal advisers where necessary.

**Providing information**

RUMMAN CARE LTD aims to ensure that individuals are aware that their data is being processed, and that they understand:

* How the data is being used
* How to exercise their rights

To these ends, the company has a PRIVACY STATEMENT, setting out how data relating to individuals is used by the company.

[This is available on request. A version of this statement is also available on the company’s website.]