Red Snapper Group

Data Protection Policy

Title	Data Protection Policy
Department	Security – Data Protection
Sector	RSG
Document Owner	Clive Brown – Data Protection Officer
Data Classification	Public
Type	Controlled
Date Adopted:	April 2018
Date of Next Review:	November 2022

Version Control – Controlled Document

Owner	Version No.	Saved As	Date	Changes Made
Ryan Farmer	v1.	Data Protection Policy v1.	Apr-18	Draft Created
Ryan Farmer	v1.	Data Protection Policy v1.	May-19	Review of document information
Ryan Farmer	v2	Data Protection Policy v2.	Sep-20	Front cover and version control box created
Ryan Farmer	v2.1	Data Protection Policy v2.1	Sep-20	Retention periods updated
Ryan Farmer	v2.2	Data Protection Policy v2.2	Oct-20	Individual policies merged to create group document
Lauren Moore	v3.	Data Protection Policy v3.	Apr-21	New designated policy owner confirmed. Updated policy layout
Clive Brown	v4.	Data Protection Policy v4.	Jun 21	Updated whole document
Clive Brown	V4.1	Data Protection Policy v4.1	Nov 21	Updated section 4.3 – Criminal Records

Table of Contents

1. Introduction 4
2. Meanings 4
2.1 Personal Data 4
2.2 Processing 4
2.3 Controller 4
2.4 Processor 4
3. The UK-GDPR key Principles 4
3.1 Lawfulness, fairness and transparency 5
3.2 Purpose limitation 5
3.3 Data minimisation 5
3.3 Accuracy 5
3.4 Storage limitation 5
3.5 Integrity and confidentiality (security) 5
3.6 Accountability 5
4. Conditions for processing personal data 5
4.1 Lawful basis of processing 5
4.2 Special categories of personal data 6
4.3 Criminal Records 6
5. Individual Rights 6
5.1 Individual Rights procedures 7
5.2 Freedom of Information Requests 7
5.3 Environmental Information Regulations 7
6. Personal Data Breach 7
6.1 Personal Data Breach procedures 8
7. Data Protection Impact Assessments 8
8. Our commitment to data protection 8

1. Introduction

In order to operate efficiently, we must collect, use and store (process) personal data about people with whom we work. These may include members of the public, current, past and prospective employees, jobseekers, funded bodies, and suppliers. In addition, we may be required to collect and use personal data in order to comply with legal requirements.

All personal data we process must be handled properly, and we must comply with Data Protection Regulations and Laws. This includes the UK General Data Protection Regulation (UK-GDPR), the Data Protection Act 2018 (DPA-2018), the Privacy and Electronic Communications Regulations (PECR) and Information Commissioners (ICO) Guidance. The UK-GDPR and the DPA-2018 provide rights to people whose personal data we may hold.

We consider that the correct treatment of personal data is integral to our successful operations and to maintaining trust of the persons we deal with. We fully appreciate the underlying principles of the Regulations and Laws and support and adhere to their provisions.

We are registered with the ICO as a data controller and also process personal data we control.

We also process and sometimes control personal data on behalf of our clients for which we should be aware.

2. Meanings

2.1 Personal Data

Means 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 that data subject.

2.2 Processing

Means any operation performed on personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.3 Controller

Means the Red Snapper legal entity or often a public authority, who alone or jointly determine the purposes and means of the processing of personal data.

2.4 Processor

Means the Red Snapper legal entity or often a public authority which processes personal data on behalf of the controller.

3. The UK-GDPR key Principles

The UK GDPR sets out key principles relating to processing of personal data, these are;

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation

- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

3.1 Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

3.2 Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.3 Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

3.3 Accuracy

Personal data should be accurate and kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate rectified or erased without delay.

3.4 Storage limitation

Personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which it is processed.

3.5 Integrity and confidentiality (security)

Personal data must be 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.

3.6 Accountability

The controller is responsible for, and should be able to demonstrate compliance with these key principles.

4. Conditions for processing personal data

4.1 Lawful basis of processing

We will ensure that at least one of the following conditions is met before we process any personal data:

1. The data subject has consented to the processing.
2. The processing is necessary for the performance of a contract with the data subject.
3. The processing is required under a legal obligation.
4. The processing is necessary to protect vital interests of the data subject.

5. The processing is necessary to carry out public functions e.g. administration of justice.
6. The processing is necessary in order to pursue our legitimate interests or those of third parties (unless these interests are overridden by the interests of the data subject).

4.2 Special categories of personal data

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation is not allowed unless one of the following applies;

- The data subject has given explicit consent to the processing of the personal data for one or more specified purposes.
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.
- Processing relates to personal data which has been manifestly made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of legal claims.
- Processing is necessary for reasons of substantial public interest.
- Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee.
- Processing is necessary for reasons of public interest in the area of public health.

Special categories of personal data are also affected by requirements in the DPA-2018.

4.3 Criminal Records

The processing of criminal records can only be undertaken when certain conditions apply as provided for in the DPA-2018. Before any criminal records processing is undertaken, a Data Protection Impact Assessment must be undertaken and usually an Appropriate Policy Document completed as well. These should be signed off by compliance and or the Data Protection Officer before processing is started.

5. Individual Rights

We will ensure that individuals are given their rights under the legislation including:

1. The right of access to their personal information.
2. The right to rectification of inaccurate data.
3. The right to erasure (‘right to be forgotten’).
4. The right to restriction of processing.
5. The right to data portability.
6. Right to object to processing.

7. The right not to be subject to a decision based solely on automated processing, including profiling.

5.1 Individual Rights procedures

When we receive an Individual rights request from a data subject we must take action.
The request should be forwarded to the DPO inbox dpo@redsnappergroup.co.uk. The request will be reviewed to determine which business or client the request belongs to.

If the request belongs to a client, the request will be forwarded to the client if the agreement with the client determines this. A receipt of the individual rights request will be issued and retained.

If the request belongs to a Red Snapper business, the request is forwarded to the responsible person in that business to take the appropriate actions.

If the request belongs to a client but Red Snapper is obliged to undertake the action to deal with the request, then the responsible person will undertake that action.

All Individual rights requests must be referred to the Data Protection Officer for guidance concerning the action to be taken.

All requests are to be actioned within one month of receipt, and are to be logged in the Individual Rights log.

5.2 Freedom of Information Requests

Organisations that Red Snapper provide a service to may be subject to the requirements of the Freedom of Information Act.

If a Freedom of Information (or FOI) request is received it should be forwarded to the DPO inbox dpo@redsnappergroup.co.uk, after which it will be assessed and forwarded to the relevant client if appropriate.

Often these requests are an Individual Rights Request and subject to the UK-GDPR.

5.3 Environmental Information Regulations

Organisations that Red Snapper provide a service to may be subject to the requirements of the Environmental Information Regulations.

If an Environmental Information Regulations request is received it should be forwarded to the DPO inbox dpo@redsnappergroup.co.uk after which it will be assessed and forwarded to the relevant client if appropriate.

Often these requests are an Individual Rights Request and subject to the UK-GDPR.

6. Personal Data Breach

The UK-GDPR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

6.1 Personal Data Breach procedures

Where a potential personal data breach is identified, we have 72 hours (if the breach is reportable) to report the breach to the Information Commissioners Office.

If you think you have identified a personal data breach you should take immediate action to stop or mitigate the breach.

Details of the potential breach should be forwarded to a Director who will review the breach and determine which business or client the breach is relevant to.

If the breach is relevant to a client, the details of the breach will be notified to the client if the agreement with the client determines this. A receipt of the breach report will be requested and retained.

The client will be provided with as much information regarding the breach, and any information they request will be provided without undue delay.

If the breach is relevant to a Red Snapper business, the breach information is forwarded to the responsible person in that business to take the appropriate action.

If the breach is relevant to a client but Red Snapper is obliged to undertake the action to deal with the breach, then the responsible person will undertake that action.

All potential breaches are to be referred to the Data Protection Officer for guidance without undue delay, and if reportable to the ICO must be reported within 72 hours of the breach having been identified.

Following the actions above, an assessment should be carried out to identify the reasons for the breach, and procedures put in place to mitigate risk of a repeat of the breach.

7. Data Protection Impact Assessments

The UK-GDPR states;

“Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks”.

In practice it is hard to know if a new or changed processing activity is likely to result in a high risk to the data subjects. Therefore whenever a new or changed processing activity is to be introduced a Data Protection Impact Assessment (DPIA) should be undertaken.

Screening questions will determine if the whole DPIA is to be completed.

8. Our commitment to data protection

We will ensure that:

- Everyone managing and handling personal information understands that they are responsible for following good data protection practice.
- There is someone with specific responsibility for data protection in the organisation.
- Staff who handle personal information are appropriately supervised and trained.
- Queries about handling personal information are promptly and courteously dealt with.
- People know how to access their own personal information.
- Methods of handling personal information are regularly assessed and evaluated.
- Any disclosure of personal data will be in compliance with approved procedures.
- We take all necessary steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.
- All contractors and other thirds parties who process personal data on behalf of Red Snapper will be required to confirm that they will abide by the requirements of Article 28 of the UK-GDPR with regard to information supplied by us.

End.