DRPG

DATA PROTECTION & PRIVACY POLICY

Version:	5
Published:	31/08/2022
Created by:	Risk Factory / James Hurley
Approved by:	Richard Parmenter
Confidentiality level:	Restricted

Contents

1 Purpose and scope

This policy has been developed to set forth minimum requirements to ensure the protection of subject data processed, stored, and transmitted by **DRPG**.

2 Responsibilities and applicability

Policies detailed herein apply to all **DRPG** companies, employees (team members), contractors and third-party suppliers, who connect to **DRPG's** information and communications technology (ICT) systems that process, store, or transmit data subject information.
The Data Protection Officer (DPO) bears the overall responsibility for monitoring and ensuring compliance for these policies.

Nonetheless, to be effective, compliance activities must be a collaborative effort involving the support of all **DRPG's** business stakeholders, team members, contractors, and third-party service suppliers.

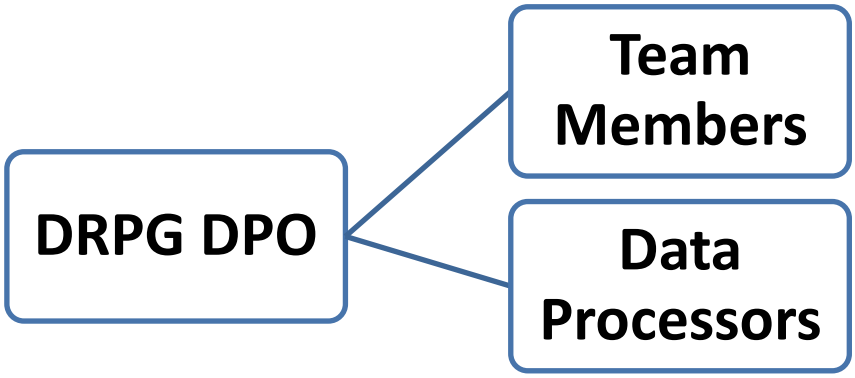
The DPO shall be responsible for:

- Conducting annual and ad-hoc audits to verify and document overall group compliance to these policies.
- Training team members, to raise awareness of Data Protection and foster a data privacy culture.
- Notifying UK Information Commissioner Office (ICO) of any suspected or confirmed breaches or any associated communication as required.
- The contact details for **DRPG's** Data Protection Officer are as follows:

Name: James Hurley
Title: Head of IT / Information Security Manager
Tel: 01299 250531
Email: dpo@drpgroup.com

The DPO shall be responsible for ensuring policies are understood and complied with, by any outsourced Data Processors. (DP) That conduct applicable assessments, compliance and liability requirements are stated in applicable contracts and service level agreements.

All users of **DRPG**'s ICT systems are responsible for properly using the security controls that are in place including technical, administrative, or other appropriate measures designed to protect subject data.



3 Referenced documents

ISO27001:2013 A…
DRPG ISMS REC 18.2 – Data Processors
DRPG ISMS REC - DPP-A2-PIA-01
DRPG 62 ISMS 18.2 – Website Privacy Policy Template
DRPG ISMS DOC 12.6 - Privacy by Design

4 Exceptions

DRPG's DPO shall have the authority to grant exceptions to the policies and procedures detailed herein. Requests for exceptions to established data protection policies and procedures shall be made in writing via email and submitted to the DPO for review and approval. The request should state the business case and/or operational obstacle prohibiting the policy or procedure from implementation and propose an alternative and appropriate "compensating control" to mitigate the associated security risk.

All exceptions require the prior written approval from the DPO, and exceptions shall be submitted using the DPA Exception Form. The record of exceptions shall be maintained by the DPO on a risk register and submitted to the ISSG meetings for reference.

5 Data Subject Definition

A "data subject" is simply defined as any person (living or dead) for which a **DRPG** company holds information.

Given this definition, it is understood that **DRPG** processes, stores and transmits both **Personal Data** and **Sensitive Personal Data** information (as defined below) associated with data subjects under the following two primary categories:

- Team members
- Client data (Third party data)

Personal Data and **Sensitive Personal Data** associated with other data subjects however may also be processed, stored or transmitted by **DRPG**. These data subjects may include:

- Volunteers, agents, temporary and contract team members
- Suppliers and their employees
- Complainants, correspondents and enquirers
- Relatives, guardians and associates of other data subjects
- Advisers, consultants and other professional experts
- Students and pupils and apprentices
- Press media
- Offenders and suspected offenders
- Healthcare, social and welfare advisers or practitioners

Personal Data and **Sensitive Personal Data** shall be subject to the applicable controls stated herein regardless of the data subject.

6 Data Subject Information Classification

DRPG identifies the following categories of data as being subject to protection:

"**PERSONAL DATA**" Personal data is any information that can be used to identify or distinguish one data subject (see below) from another or by combining the information with other information that you have or are likely to have in the future.

Examples of Personal Data are:

- A data subject's name, address, date of birth
- A data subject's physical description, height weight, colour of hair or eyes
- A data subject's driver's license
- A data subject's personal or national insurance number

"**SENSITIVE PERSONAL DATA**" Sensitive personal data is any personal information that could be used in a discriminative way and is likely to be of a private nature.

Examples of Sensitive Personal Data are:

- A data subject's medical condition details
- A data subject's racial or ethnic origin
- A data subject's political opinions
- A data subject's religious, or other similar beliefs
- A data subject's physical or mental health or condition
- A data subject's sexual orientation
- A data subject's criminal convictions or alleged criminal acts

Questions or clarifications regarding these definitions should be referred to the DPO for resolution.

7 Information Marking Scheme

All data subject information classified as Personal Data (and not containing Sensitive Personal Data must be clearly marked "**RESTRICTED**".
All data subject information classified as Sensitive Personal Data must be clearly marked "**CONFIDENTIAL**".
This requirement applies to any/all forms that the data may take in all states to include: hardcopy, applications used for processing, storage and electronic mail in use, in transit or at rest.

8 Data Processor Definition

A "Data Processor" is simply defined as any natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
DRPG shall ensure that the Data Processor complies with GDPR.
A list of Data Processors can be found in *DRPG ISMS REC 18.2 – Data Processors*

9 Ownership of Customer Subject Data

DRPG owns its customer databases and the information contained therein.
Subject data collected may be processed, stored or transmitted by **DRPG**-approved Data Processors subject to its protection in accordance with the policies.

10 Policy Framework

To ensure the appropriate protection of subject data that is processed, stored and transmitted, **DRPG** shall adhere to the policies stated in this section.

Policies shall be implemented at all **DRPG** (and **DRPG** Appointed Data Processors) operating locations and apply to both categories of information (Personal Data and Sensitive Personal Data) unless where otherwise noted.

10.1 Principles

DRPG shall ensure that all subject data processed, stored or transmitted is:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and where necessary, kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

- 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.

10.2 Lawful Basis of Processing

10.2.1. Consent

It is **DRPG**'s policy that **Personal Data** and **Sensitive Personal Data** shall not be processed without a business reason and without prior consent from the data subject.

Forms used to collect information from data subjects directly which are deemed **Sensitive Personal Data** shall require the data subject's active consent.

DRPG shall implement a process to allow data subjects the option to deny the right to process their **Sensitive Personal Data**.

If requested, **DRPG** shall provide written assurance to data subjects that they do not process, store or transmit their **Sensitive Personal Data**.

All communications to **DRPG**'s clients (to include emails and text messages) shall request the clients "opt-in" consent for **DRPG** to process their information, consent is used as the lawful basis of processing.

DRPG must obtain end user active consent, prior to placing "cookies" in their browsers.

All **DRPG** team members must give consent for **DRPG** to process, store and transmit information associated with their employment.

Where the processing of **DRPG**'s team member information is carried out by a third party, applicable service level agreements shall be required, for **DRPG** to process, store and transmit information, associated with their employment. Note: If the third party is unwilling or unable to agree to this requirement, the information should be withheld. Information provided to third party organisations is only allowed to be used by those companies in connection with the product or service contracted and will be subjected to **DRPG**'s third party vetting process.

10.2.2 Contract

DRPG shall collect and process personal data without explicit consent if it is required to fulfil a contract with the data subject, where the contract cannot be completed without the personal data in question.

10.2.3 Legal Obligation

DRPG shall collect and process personal data without explicit consent if it is required to comply with the law.

10.2.4 Vital Interests

DRPG shall collect and process personal data if it is required to protect the vital interests of the data subject or of another natural person.

DRPG shall retain documented evidence with the DPO.

10.2.5 Public Tasks

DRPG shall process data if it needs to perform a task that is in the public interest or as part of an official duty.

DRPG shall retain documented evidence with the DPO.

10.2.6 Legitimate Interests

DRPG shall process specific personal data for the legitimate interest of the company if the rights and freedom of the data subject are not affected in a significant way.

DRPG shall carry out a Legitimate Interest assessment where appropriate.

10.3 Individual Rights

10.3.1 Rights to be informed

DRPG shall ensure that the data subject is informed about the use of their data and their rights over it.

All **DRPG** properties (and websites) shall post a "Privacy Notice" clearly stating the purpose of their data collection activities.

Please see the DRPG 62 ISMS 18.2 – Website Privacy Policy Template.

10.3.2 Right to Access

It is **DRPG**'s policy to allow data subjects to access the personal data we hold on them. Subjects requiring access to their information must fill out and submit a Subject Access Request (SAR), please email ***dpo@drpgroup.com*** to request a SAR form.

DRPG shall be responsible for responding to SARs within thirty (30) days of receipt.

At a minimum, **DRPG**'s responses to SARs shall include:

- A description of the Personal Data held

- The purposes for which the information is used or will be used (e.g. marketing, service reminders etc.)
- The sources of the information (e.g. from where **DRPG** obtained the information)
- Recipients or classes of recipients to whom the information is or may be disclosed

Team members shall consult the DPO if they require assistance on responding to a SAR.

10.3.3 Right to Rectification

It is **DRPG**'s policy to allow data subjects to rectify their personal data we hold on them if it is inaccurate or incomplete.

Where possible, **DRPG** shall ensure that each of the recipients to whom the personal data is disclosed are informed of the rectification.

DRPG shall respond to the rectification request within one month (30 days).

Appropriate measures shall be implemented by **DRPG** to ensure all Personal Data and Sensitive Personal **Data** processed, stored or transmitted is accurate and kept up to date on a regular basis.

10.3.4 Right to Erasure

DRPG shall ensure that the personal data of the data subject, shall be erased when the personal data is no longer necessary, for the purpose for which it was collected.

DRPG shall ensure that personal data is erased if the data subject withdraws consent and there is no basis for continued processing. Please contact ***dpo@drpgroup.com*** to request a consent withdrawal form.

DRPG shall erase the personal data if the data subject objects to the processing of the data.

DRPG shall only retain personal data if it is reasonably required for the purpose(s) for which it was collected.

10.3.5 Right to Restrict Processing

DRPG shall ensure that the data subject has the right to restrict the processing of their personal data if the data is not accurate.

DRPG shall ensure that the data processing is restricted if the processing is unlawful.

DRPG shall decide on each request by involving the DPO.

10.3.6 Right to Data Portability

DRPG shall ensure the personal data of the data subject is provided to them in a structured, commonly used and machine-readable format.

DRPG shall ensure the transfer to another party if requested by the data subject.

10.3.7 Right to Object

DRPG shall ensure that the data subjects have the right to object to processing, based on legitimate interest.

DRPG shall ensure that the data subjects have the right to object to direct marketing.

10.3.8 Rights Related to Automated Decision Marking including Profiling

DRPG shall ensure that the data subject has the right to not be the subject of automated decision-making, where the decision has a significant effect on them.

10.4 Accountability & Governance

10.4.1 Contracts

DRPG shall ensure that all contracts that involve the processing of personal data shall be subject to a document contract that includes the specific information and terms required by the GDPR.

10.4.2 Documentation

DRPG shall ensure that documentation are maintained for data processing activities, data sharing and data retention.

DRPG shall ensure that records are up to date and reflect current processing activities.

10.4.3 Data Protection by Design & Default

DRPG shall ensure the adoption of privacy by design and default for all new and significantly changed systems that collect and process personal data.

For more information, see DRPG ISMS DOC 12.6 - Privacy by Design.

10.4.4 Data Protection Impact Assessments

DRPG team members, must complete a Privacy Impact Assessment (PIA) for new projects involving the processing, storage or transmittal of data subject information.

PIAs should be completed and submitted to the DPO, for review and approval.

For more information, see DRPG ISMS REC - DPP-A2-PIA.docx

10.5 Security

It is **DRPG**'s policy to provide appropriate security to ensure the protection of both **Personal Data** and **Sensitive Personal Data** that it processes, stores or transmits.

Information processed on **DRPG** systems shall be protected in accordance with the current published **DRPG** information security policies and procedures.

3rd party systems that are used to host, process, store or transmit **DRPG Sensitive Personal Data** howsoever, shall meet or exceed the following safeguards:

- Systems shall be protected from unauthorised external access (firewalls).
- System devices shall be protected by firewalls and anti-malware protection.
- Operating systems and applications shall be configured with latest security patches and updates.
- Data shall be encrypted when at rest where appropriate (stored) and password protected.
- Data shall be encrypted, and password protected when in transit (electronically).
- Data shall be backed up regularly and back-ups encrypted and stored in off-site location.
- Data shall be securely removed before disposal of devices.

Additionally, procedures should be implemented to ensure:

- Access to information is restricted to a "need to know" basis.
- Passwords to devices accessing information meet or exceed published **DRPG** requirements
- Hardcopy information is marked and shredded when no longer required.
- Hardcopy information is stored in locked containers in alarmed offices

It should be noted that these minimum safeguards detailed herein apply to computing systems regardless of technology (wireless, software as a service, VoIP, virtualised or public, private or hybrid cloud computing etc.).

All personnel with access to **DRPG** systems that process the Privacy Data that includes the **Sensitive Personal Data**, shall be required to:

- receive data protection awareness training prior to being granted access
- receive regular security awareness briefings designed to heighten their information security awareness and remind them of their on-going security responsibilities

10.6 International Transfers

DRPG can transfer **Personal Data** and **Sensitive Personal Data** from the UK to non-EU countries. However, data transmittal, processing and storage must meet or exceed requirements stated herein.

DRPG shall obtain consent from the applicable data subject when transferring their **Sensitive Personal Data** outside the EU.

Sensitive Personal Data shall not be transferred to a country or territory outside the European Union (EU) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

DRPG shall ensure via contractual obligations that **Sensitive Personal Data** does not exit the EU without legitimate business or legal purposes and this must be ensured from a contractual standpoint.

Where processing across more than one national boundary is undertaken, it is necessary to determine which national law applies to which processing operation.

10.7 Personal Data Breaches

As soon as **DRPG** becomes aware that a personal data breach has occurred which is likely to risk a data subject's rights, **DRPG** shall notify the Information Commissioner's Office (ICO) without undue delay and where feasible, not later than 72 hours.

Where the notification to the ICO is not made within 72 hours, **DRPG** shall report the reason for the delay.

When personal data breach is likely to result in a high risk to the rights and freedom of the data subject, **DRPG** shall communicate the breach to the data subject without undue delay.

DRPG shall document any personal data breach, comprising the facts relating to the breach, its effect and the remedial action taken.

11 Document owner and validity

The ISM is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements of the ISMS.

This document is valid from 31/08/2022

Next review date 26/08/2023

12 Change Record

Issue	Description of change	Approved by	Date
0.1	First draft of updated GDPR Data Protection Policy	James Hurley	01/04/2018
1	Aligned to drp branding and published	James Hurley	01/05/2018
2	Annual review of policy and updated to DRPG branding	James Hurley	08/05/2019
3	Annual review of policy. Updated all links to external documents and removed default privacy policy. Inserted link to new website privacy policy.	James Hurley	02/10/2020
4	Annual review and update to published date. Incorrect date previously entered.	James Hurley	06/09/2021
5	Annual Review	James Hurley	31/08/2022