Data Protection Policy

Table of contents

Introduction

This policy provides information and guidelines on the proper handling of Personal Data, which will help PRI treat individuals' Personal Data with respect and help us to build good relationships with our signatories, suppliers and other stakeholders.

You must comply with this policy from the 'approved by date' as stated in the 'version information' at the end of this document, and with any updates made to it, as from the date such updated policy is made available to you.

This policy is one of a number of documents and policies which relate to the handling of Personal Data. These policies can be found on the PRI Policies page in SharePoint and must be consulted, as necessary.

Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the PRI's Disciplinary Policy. Significant or deliberate breaches of this policy, such as accessing or using data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

Updating

This policy will be reviewed and updated at least annually. New versions will be published on the dedicated policy SharePoint page. You will be notified of any amendments to this policy via PULSE.

1 Definitions

In this policy:

Controller	means the person who alone or jointly determines the purposes for which, and the means by which, any Personal Data is Processed. In most cases, PRI will be a Controller for the Personal Data it Processes;
Data Subject	means the identified or identifiable living individual to whom Personal Data relates;
DPA	means data protection authority;
DPIA	means a data protection impact assessment, being an assessment of any privacy risks associated with high-risk Processing of Personal Data by PRI and any processes and controls in place to mitigate or eliminate such risks;
EU GDPR	means regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data;
Group Company	means in relation to a company, any subsidiary or holding company from time to time of that company, and any subsidiary from time to time of a holding company of that company;
HR-related Personal Data	means Personal Data of PRI job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees;
Personal Data	means information relating to an identified or identifiable natural person;
PRI	Means PRI Association, incorporated and registered in England and Wales with company number 07207947 together with its Group Companies;
Processing	means 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, the terms Processed and Process should be read in line with this;
Processor	means any natural or legal person, public authority, agency or other body who Processes Personal Data on behalf of a Controller;
Special Category Data	means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used to uniquely identify an individual, data concerning health or data concerning a natural person's sex life or sexual orientation;
UK GDPR	means the General Data Protection Regulation, Regulation (EU) 2016/679, as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or of a part of the United Kingdom from time to time).

2 Other defined terms

In this policy, any reference to the terms "**we**," "**us**" and "**our**" refer to PRI.

3 Scope

This policy applies to all Processing of Personal Data by PRI, except for Processing of HR-related Personal Data. For details of how PRI Processes HR-related Person Data, please see the PRI Employee Handbook.

All employees, consultants, and contractors who process Personal Data on behalf of the PRI are obliged to comply with this policy.

4 The data protection principles

PRI operates in multiple countries across the world. The requirements and procedures set out in this policy apply to PRI's operations in all locations. We must all comply with all applicable laws when handling Personal Data, including the data protection principles set out in the EU GDPR and the UK GDPR and any local laws that impose additional requirements on the PRI. If you have any questions about local laws, please contact the PRI's General Counsel.

4.1 **Lawfulness, fairness and transparency**

Personal data must be Processed lawfully, fairly and in a transparent manner.

4.1.1 The requirements

(a) Under the EU GDPR and the UK GDPR, we must not Process Personal Data unless one of the legal bases set out in the EU GDPR or the UK GDPR (as applicable) applies.

(b) We must always identify and document the legal basis which permits Processing.

(c) We must ensure that use of Personal Data is fair and is not unduly detrimental, misleading or unexpected.

(d) We must ensure that individuals receive clear, easy to understand information about how we Process their Personal Data when the Personal Data is collected.

4.1.2 How do we comply?

(e) PRI maintains a record of Processing activities, which records the legal bases of Processing operations.

(f) We use privacy assessments to ensure that Processing is carried out in compliance with our obligations under applicable data protection legislation and to undertake a DPIA where this is required by applicable data protection legislation or where it would be good practice to do so. We undertake these assessments to ensure that our use of Personal Data is lawful, fair and transparent. See Section 11 (*Privacy Assessments*) for more information.

(g) We undertake Legitimate Interest Assessments (**LIAs**) to check that our interests for Processing are not overridden by the interests of the Data Subject.

(h) We provide privacy notices to Data Subjects at the point of Personal Data collection.

(i) We review issues of lawfulness, fairness and transparency on a regular basis as part of the checks referred to at 4.7.2(f) below.

4.2 **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.

4.2.1 *The requirements*

(a) Personal Data must be used only in accordance with the purposes that have been notified to Data Subjects at the point of collection of the Personal Data.

(b) We must assess any new use of Personal Data to ensure it is compatible with the original, notified, purposes or if we have the Data Subject's consent to the new purpose or a clear provision set out in law allowing/requiring Processing for the new purpose.

4.2.2 How do we comply?

(a) We specify the purposes of Processing in all relevant privacy notices.

(b) We carry out regular reviews of Processing activities to ensure that Processing continues to be consistent with the purposes notified to individuals as part of the checks referred to at 4.7.2 (f) below.

(c) When starting new projects involving Personal Data, we carry out a privacy assessment including a DPIA where necessary to ensure that any new use of data is compatible with the purposes notified to individuals. See Section 11 *(Privacy Assessments)* for more information.

4.3 **Data minimisation**

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is Processed.

4.3.1 The requirements

(a) We must ensure that we only collect and use the Personal Data that is necessary for the purpose of the Processing activity in question.

(b) We must use sufficient Personal Data to fulfil our specified purposes.

(c) We must ensure there is a rational link between the Personal Data Processed and the specified purpose.

4.3.2 How do we comply?

(a) We review data collection activities on a regular basis as part of the checks referred to at 4.7.2 (f) below.

(b) When starting new projects, we carry out a privacy assessment which takes into account data minimisation requirements. See Section 11 *(Privacy Assessments*) for more information.

4.4 **Accuracy**

Personal Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

4.4.1 The requirements

(a) We must use appropriate measures to check that data is accurate and up to date as well as processes which allow us to amend/update inaccurate Personal Data.

(b) If we are informed of inaccurate data, we must ensure that our records are updated promptly where it is appropriate to do so.

(c) If an individual challenges the accuracy of Personal Data, we must have processes in place to manage this.

4.4.2 How do we comply?

(a) Each team must check that Personal Data is accurate at the point of collection and thereafter is kept up to date.

(b) We review Personal Data accuracy on a regular basis as part of the checks referred to at 4.7.2 (f) below.

(c) We have policies and procedures in place to deal with requests for erasure and rectification made by Data Subjects.

(d) We ask employees to check the accuracy of their records on a regular basis.

4.5 **Storage limitation**

We must not keep Personal Data for longer than we need it for the purposes for which the Personal Data is Processed.

4.5.1 The requirements

(a) We must ensure that Personal Data is kept for no longer than necessary and that Personal Data is securely destroyed, deleted or anonymised when it is no longer needed.

4.5.2 How do we comply?

(b) We have a Data Retention Policy which specifies retention periods for the Personal Data we hold. Retention periods are regularly reviewed to ensure they are appropriate.

(c) Each team must comply with the Data Retention Policy and ensure any team retention periods are included in the Data Retention Policy.

(d) We have policies and procedures in place to deal with requests for erasure made by Data Subjects.

(e) We review Personal Data retention on a regular basis as part of the checks referred to at 4.7.2 (f) below.

4.6 **Integrity and confidentiality (security)**

We must ensure that we have appropriate security measures in place to protect Personal Data, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage.

4.6.1 The requirements

(a) We must put in place appropriate security measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

(b) We must ensure that all employees understand and comply with the Information Security Policy and associated policies.

4.6.2 How do we comply?

(a) We have an Information Security Policy which sets out our expected standards in relation to information security matters.

(b) PRI's Technology & Infrastructure team is responsible for information security policies.

(c) Each team is responsible for ensuring that all policies relating to information security which are applicable to that team are followed.

(d) When commencing new projects, we carry out a privacy assessment to ensure that the proposed Processing is risk assessed with regard to the

security of the Processing. See Section 11 *(Privacy Assessments)* for more information.

(e) We have mandatory, annual, information security training for employees.

(f) We review compliance with the Information Security Policy on a regular basis as part of the checks referred to at 4.7.2 (f) below.

4.7 **Accountability**

We are responsible for, and must be able to demonstrate compliance with, EU and UK GDPR including the principles set out in Sections 4.1 to 4.6 above.

4.7.1 The requirements

(a) We must ensure we take responsibility for compliance with data protection legislation at the highest management level and throughout our organisation.

(b) We must be able to demonstrate compliance with data protection legislation.

(c) We must maintain a record of all Processing activities.

(d) We must implement appropriate security measures.

(e) We must take a data protection by design and default approach, meaning that we ensure data is protected by default and data protection is actively addressed as a matter of course in the running of our organisation and the provision of our services.

(f) We must ensure that appropriate policies and processes are in place and review them at regular intervals.

(g) We must undertake regular checks to monitor compliance with policies and processes and take action to ensure that any issues of non-compliance are remedied.

(h) We must put in place written contracts with third parties who Process Personal Data on our behalf.

(i) We must complete DPIAs for high-risk Processing activities.

(j) We must record and where required, report, Personal Data Breaches.

4.7.2 How do we comply?

(a) We have undertaken a documented assessment and concluded that we are not legally obliged to appoint a Data Protection Officer. This decision is kept under review. We have appointed the General Counsel to be responsible for data protection within our organisation.

(b) The General Counsel maintains a programme of work that includes key data protection activities and is supported by external data protection advisers who provide expert advice and additional resource.

(c) We have policies and procedures in place as set out in on the PRI Policies page on SharePoint.

(d) We have a ROPA. See Section 12 (*Record of Processing Activities*) for more information.

(e) We undertake DPIAs where Processing is "high risk". See Section 11 (*Privacy Assessment)* for more information.

(f) The General Counsel ensures that regular checks are undertaken to check that data protection requirements are being met in practice.

(g) We review policies annually. This is included in the programme of work.

(h) We put in place written contracts with third parties who Process Personal Data on our behalf.

(i) We put in place suitable arrangements for data governance.

5 Legal bases for Processing Personal Data

5.1 The EU GDPR/UK GDPR sets out the following legal bases for Processing Personal Data:

5.1.1 Consent: the individual has given clear consent for us to Process their Personal Data for a specific purpose.

5.1.2 Contract: the Processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

5.1.3 Legal obligation: the Processing is necessary for us to comply with the law (not including contractual obligations).

5.1.4 Vital interests: the Processing is necessary to protect someone's life.

5.1.5 Public task: the Processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

5.1.6 Legitimate interests: the Processing is necessary for our legitimate interests or the legitimate interests of a third party unless the individual's interests override those legitimate interests.

5.2 Whenever we Process Personal Data, we must identify and document the legal basis for the Processing in our Record of Processing Activities. In the case of Special Category Data, there are additional conditions which must be complied with as set out below.

6 Special Category Data

6.1 Processing Special Category Data is prohibited unless one of the conditions listed in the EU GDPR and/or the UK GDPR (as applicable) is/are met in addition to having one of the legal bases set out in Section 5 (*Legal bases for Processing Personal Data*). These conditions are as follows:

6.1.1 Explicit consent

6.1.2 Employment, social security and social protection (if authorised by law)

6.1.3 Vital interests

6.1.4 Not-for-profit bodies

6.1.5 Made public by the data subject

6.1.6 Legal claims or judicial acts

6.1.7 Reasons of substantial public interest (with a basis in national law)

6.1.8 Health or social care (with a basis in national law)

6.1.9 Public health (with a basis in national law)

6.1.10 Archiving, research and statistics (with a basis in national law)

6.2 The Processing of Special Category Data undertaken by PRI is set out in our privacy notices.

6.3 Prior to any project which involves Processing new Special Category Data or Processing existing Special Category Data for a new purpose, we must review the Privacy Assessment Policy and accompanying procedures and identify the Article 9 UK GDPR and/or EU GDPR

as applicable) provision which is relied on as the legal basis for Processing the Special Category Data.

7 Security

7.1 We are required to take reasonable technical and organisational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.

7.2 All employees must comply with the Information Security Policy which sets out the minimum standards which must be adopted.

8 Personal Data breaches

8.1 Personal Data breaches occur when a breach of security leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data. Our Data Breach Management Policy gives examples of situations that constitute a Personal Data Breach.

8.2 Unless a Personal Data breach is unlikely to pose a risk to individuals' rights and freedoms, we will need to report it to the relevant DPA(s) within 72 hours of PRI becoming aware of the Personal Data breach.

8.3 If a breach is likely to cause a high risk to individuals' rights and freedoms, then individuals must be notified of the breach without undue delay.

8.4 There may be other time sensitive notifications required to other regulators.

8.5 **If you suspect a Personal Data Breach has occurred, you must act immediately to inform the Technology & Infrastructure Team and PRI's General Counsel in accordance with our Data Breach Management Policy.**

8.6 The General Counsel will review the nature of the Personal Data breach, carry out an investigation and determine matters including:

8.6.1 whether the Personal Data breach needs to be notified to a DPA or to individuals,

8.6.2 whether the mitigation measures taken/proposed to be taken are appropriate,

8.6.3 if we have effectively put in place the mitigation measures proposed,

8.6.4 whether the processing can proceed or a referral to the relevant DPA is necessary.

8.7 We maintain a log of all Personal Data breaches and make this log available to the relevant DPA upon request.

8.8 **If there is an obligation to notify a DPA or individuals of a Personal Data Breach, the notification must be made by or approved in advance by the General Counsel.**

9 Sharing Personal Data

9.1 When we collect Personal Data, we must be clear, open and honest about how we use the Personal Data. This includes informing individuals about any sharing of the Personal Data and our reasons for doing so.

9.2 Sharing Personal Data requires planning and risk assessment. As such, when sharing Personal Data, we must act in accordance with our Data Sharing Policy and accompanying procedures, which detail the steps which we must take to ensure our Personal Data sharing is compliant with UK GDPR and EU GDPR (as applicable).

9.3 Please see Section 15 (*Third Party Processors*) of this policy for details about data protection requirements when we use Processors to Process Personal Data.

10 Transferring Personal Data overseas

10.1 The UK GDPR and the EU GDPR and accompanying guidance stipulate certain conditions which must be met before transferring Personal Data outside of the EEA/and/or the UK.

10.2 If you are planning to send Personal Data outside of the EEA and/or the UK, you must refer to the General Counsel for guidance on how to do this in a compliant way.

11 Privacy Assessments

11.1 If we undertake any new projects using new Personal Data or using existing Personal Data for a new purpose, we must follow the Privacy Assessment Policy and undertake a privacy assessment.

11.2 Our Privacy Assessment Policy requires that:

11.2.1 all new projects are assessed using the procedure in the Privacy Assessment Policy to determine:

(a) the nature and scope of the Processing

(b) the legal basis for the Processing

(c) whether there is any Processing which is likely to result in a high-risk to the rights and freedoms of individuals

(d) actions which need to be taken to ensure the Personal Data is handled in a manner that is compliant with applicable data protection legislation (by means of a DPIA or Privacy Compliance Check as relevant)

11.2.2 if Processing is likely to result in a high risk to the rights and freedoms of individuals, we must undertake a DPIA. The DPIA will record the Processing operations and the purposes of the Processing. It will include an assessment of the necessity and proportionality of the Processing and an assessment of the risks to the individuals and the measures that have been/will be taken to mitigate those risks.

11.2.3 a DPIA must be conducted prior to commencement of the Processing;

11.2.4 mitigating actions identified in a DPIA must be taken to address risks; and

11.2.5 in cases where a high risk cannot be mitigated, PRI must consult the relevant DPA.

12 Record of Processing Activities (ROPA)

12.1 The PRI's ROPA contains various details of each Processing activity, such as the Personal Data involved, what the operation is, whose data is used, where it is stored, whether a Processor is involved etc.

12.2 Any new Processing or changes to Processing activities must be recorded and we must put in place a process to regularly review the ROPA to ensure that it is accurate and up to date.

12.3 Each team is responsible for reviewing and updating the record for their team/department annually and, whenever there is a change in Processing activities.

12.4 Privacy assessments may identify situations in which the ROPA needs to be updated.

13 Training

13.1 We must ensure that all employees receive adequate training to enable them to comply with this policy and any applicable data protection laws. Employees must complete data protection and information security training during their induction and at least annually thereafter.

14 Marketing

14.1 We use Personal Data to market our products, services and events to individuals. This is known as direct marketing.

14.2 Whilst EU GDPR/UK GDPR applies to direct marketing which uses Personal Data, there is also other legislation which must be complied with where applicable.

14.3 When we use Personal Data for direct marketing purposes, we make sure that this is done in a compliant way. In particular we make sure that:

14.3.1 The legal basis for the marketing is compliant with all relevant data protection legislation;

14.3.2 Individuals can opt out of marketing at any time, free of charge, for example clicking an unsubscribe button on an email;

14.3.3 Where an individual gives consent to direct marketing, we must make sure it is as easy to withdraw consent as it was to give.

14.4 Each marketing communication must provide contact details of the Controller (most likely us) and clear information to enable individuals to opt out.

15 Third party Processors

15.1 Third parties who Process Personal Data on our behalf are known as Processors. We use Processors to help us run our organisation, for example, we use external suppliers who provide services such as payroll and IT services.

15.2 We must only use Processors who can provide sufficient guarantees to ensure that the Processing they undertake meets the requirements of EU GDPR and the UK GDPR (as applicable), and individuals' rights are respected.

15.3 We must carry out due diligence on Processors during onboarding and on an ongoing basis to ensure that they have appropriate measures in place to enable them to comply with the EU GDPR and the UK GDPR (as applicable).

15.4 Agreements with Processors must be in the form of written contracts which include mandatory clauses set out in the EU GDPR and the UK GDPR (as applicable).

15.5 Our Procurement Policy and accompanying procedures must be followed by teams when onboarding Processors and managing relationships with them.

16 Complaints

16.1 We treat complaints about our Processing of Personal Data in a serious and timely manner. Complaints from PRI employees will be dealt with by the People & Culture team and the General Counsel. Complaints from signatories or other third parties will be dealt with by the General Counsel.

17 Rights of individuals

17.1 Data Subjects have a number of rights under data protection law. These are summarised below. It is important to note that most of these rights are not absolute and not all rights apply to all the Processing we undertake. If we receive a request in relation to any of these rights, we need to respond promptly (within one calendar month) and appropriately, by following the procedures set out in the Data Subject Rights Policy and procedures.

17.2 If you receive a request from an individual to exercise one of the rights below, you should contact the General Counsel immediately for guidance on how to respond.

17.2.1 Right to be informed

Individuals have a right to be informed about how we will collect and use their Personal Data. This information must be provided to individuals in a concise, transparent, intelligible, and easily accessible format, using clear and plain language.

17.2.2 Right of access to Personal Data

Individuals have a right to:

(a) obtain confirmation that we are Processing their Personal Data;

(b) a copy of their Personal Data; and

(c) information on how we use their Personal Data.

17.2.3 Right to have inaccurate Personal Data rectified

Individuals have a right to have any inaccurate or incomplete Personal Data rectified/completed.

17.2.4 Right to have Personal Data erased

Individuals have a right to request that certain information held by us is erased. This is also known as the right to be forgotten.

17.2.5 Right to restrict Processing of Personal Data

Individuals have a right to restrict the Processing of their Personal Data in certain circumstances.

17.2.6 Right to data portability

In certain circumstances individuals can request a copy of their Personal Data in a commonly used electronic format.

17.2.7 Right to object to Processing of Personal Data

Individuals have a right to object to Processing being carried out by PRI in certain circumstances. In most cases, the right is not absolute, save in relation to situations where we are Processing Personal Data for direct marketing purposes.

17.2.8 Right not to be subject to automated decisions

Individuals have a right not to be subject to a decision which is based solely on automated Processing, including profiling, which will produce legal effects or similarly significant effect on the individual. Such decisions might include whether to enter into a contract with an individual or a decision about whether to hire an individual.

If you wish to discuss the contents of this policy or have any questions or queries regarding privacy or data protection, please contact the PRI's General Counsel.

18 Accountability and Implementation

- This Data Protection Policy is approved by the Executive Team.
- Implementation of and adherence to the policy is the responsibility of all PRI employees, consultants and contractors.
- Operational management of the Data Protection Policy will be the responsibility of the General Counsel.
- The Chief Operations and People Officer will be ultimately accountable for its execution and effectiveness.

Version no.	Approved by	Owner	Approved by date	Date last updated or reviewed	Review frequency	Next review date

1.01	Digital Transformation Executive	Security Consultant	August 2023	August 2023	Every 2 years	August 2025
2	Executive Team	General Counsel	16 December 2024	16 December 2024	Annually	Dec 2025