Data Protection Policy 2023

Purpose

The purpose of the Data Protection Policy is to ensure Ranplan and its team members, contractors and any associated third-party providers are aware of the responsibilities associated with and, as such, can fully comply with the Data Protection Act 2018 (DPA). The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

This policy sets out Ranplan's commitment to ensuring that any personal data, including special category personal data is carried out in compliance with data protection law. Ranplan is committed to ensuring that all the personal data that it processes is done in accordance with data protection law. Ranplan ensures that good data protection practice is imbedded in the culture of our staff and our organisation.

Scope

This policy applies to all personal data processed by Ranplan and is part of Ranplan's approach to compliance with data protection law. All Ranplan staff are expected to comply with this policy and failure to comply may lead to disciplinary action for misconduct, including dismissal.

Responsibility for Data Protection

All team members, contractors and associated third-parties are responsible for Data Protection. Ranplan will ensure information on the responsibilities is freely available and full training is provided.

As a small business, Ranplan does not require a Data Protection Officer. Should any team member have a concern in relation to Ranplan compliance with the GDPR they should raise this with the General Manager.

Definitions

Business Purpose	The purpose for which personal data may be used by us: Recruitment, HR, administrative, financial, regulatory, payroll and business development purposes Business purposes can include the following: ➢ Compliance with our legal, regulatory and corporate governance obligations and good practice ➢ Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests ➢ Ensuring business policies are adhered to (such as policies covering email and internet use) ➢ Investigating complaints ➢ Checking references, ensuring safe working practices, monitoring and managing team access to systems and facilities and team absences, administration and assessments ➢ Monitoring team conduct, disciplinary and grievance matters ➢ Providing employment benefits, for example the company pension scheme
Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other team members, clients, suppliers and marketing / sales contacts. Personal data we gather may include: individual's contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title and CV.
Sensitive/special personal data	GDPR defines sensitive personal data as genetic and biometric data as well as data regarding racial or ethnic origin, political opinions, religious or philosophical beliefs,

	trade union membership (or non-membership), health, sex life, sexual orientation and criminal offences or related proceedings. Sensitive personal data will be strictly controlled in accordance with this policy. In most cases the processing of such data will require explicit consent to do so unless exceptional circumstances apply or it is a legal requirement, for example, to comply with legal obligations to ensure health and safety at work.

Scope and Monitoring

This policy applies to all team members, contractors and third-party providers working with Ranplan. As an individual you must be familiar with this policy and comply with its terms. Adherence to this policy will be regularly monitored to ensure compliance.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new modified policy will be circulated to the team before being adopted.

Data Protection Principles

Ranplan will adhere to the following principles in relation to Data Protection.

1. **Lawfulness, fairness, and transparency**: Processed lawfully, fairly and in a transparent manner in relation to individuals.

2. **Purpose Limitation**: Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3. **Data Minimisation**: Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

4. **Accuracy:** 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.

5. **Storage Limitation**: Personal data should only be kept in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

6. **Integrity and Confidentiality**: Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including protection against unauthorised or unlawful access to or use of personal data and the equipment used for the processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. **Accountability**: Ranplan is responsible for, and must be able to demonstrate, their compliance with all of the above-named Principles of Data Protection.

Processing Data

Ranplan must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual.

Most lawful bases require that processing is 'necessary' for a specific purpose. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data.

Ranplan will process data in accordance with the above principles at all times. Certain departments / functions require the collation, analysis, storage and processing of data. This can be for:

Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

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

Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

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

Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Processing Sensitive Personal Data

Ranplan will ensure the processing of any sensitive personal data is restricted to what is required for one or more of the six reasons for processing data as outlined above. Any queries on the correct processing of sensitive personal data should be addressed to General Manager.

Data Retention Policy

A data retention policy is a set of rules and guidelines that define how long specific types of data should be kept and how it should be securely stored. Data retention policies are intended to ensure that data is stored securely and for only as long as needed, in order to comply with laws, regulations, and contractual requirements.

Current Employees

Ranplan will collect and store electronically personal data related to employment, salary, benefits, health and emergency contact details for the entire period of employment. Please see below the retention periods post-employment.

Former Employees

Area	Detail	Retention Period	Security considerations
Occupational Health	Health surveillance reports	40 years	Stored separately and securely
	H&S training records	7 years	
	Medical reports		
	Occupational health records		
	Application forms		
HR records / Benefits	Employee records (post leaving)	6 years	Stored securely
HMRC income tax / NI	Records	6 years + 1	Stored securely
	Correspondence with HMRC		
Employee wage / salary	(Post leaving)	6 years + 1	Stored securely
Pension	Individual pension information	12 years	Stored securely
	Pension scheme		

External Candidates

Area	Detail	Retention Period	Security considerations
Employment applications (unsuccessful)	Curriculum Vitae	6 months	Stored separately and securely
	Application forms		

Other Records

Area	Detail	Retention Period	Security considerations
Occupational Health	Health surveillance reports	40 years	Stored separately and securely
Accident Book		3 years	Stored securely
Shareholder information	Contact details	Permanently	Stored securely
	Share information		
Senior Management Team	Officers of the company	Permanently	Stored securely
Customer information	Contact details	Permanently	Stored securely

Data will be held securely and separately as appropriate in line with the above retention periods. After which time it will be securely destroyed.

Individual rights

Under the UK GDPR individuals have the following rights:

- **Information Right**: Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.
- **Right of access:** Individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is commonly referred to as a subject access request or 'SAR'.
- **Right to rectification:** A right for individuals to have inaccurate personal data rectified or completed if it is incomplete.
- **Right to erasure:** The UK GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten' and is not absolute and only applies in certain circumstances. An example of when an erasure request can only be refused is if the data must be held in order to comply with a legal obligation or in relation to the contract of employment.
- **Right to restrict processing:** Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.
- **Right to data portability:** The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
- **Right to Object:** The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing.
- **Rights related to automated decision-making including profiling:** The UK GDPR has provisions on:
    - automated individual decision-making (making a decision solely by automated means without any human involvement); and
    - profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

Sharing Data with a Third party

Ranplan will never share information with third parties for their own purposes, unless this is explained at the time the data is collected, express permission is given, or Ranplan is legally required to do so. For example, Ranplan is legally required to provide data to HMRC in relation to earnings for tax and National Insurance purposes.

Ranplan also use suppliers known as 'data processors' to process data, for example, to manage the company pension scheme. When enlisting the services of such suppliers the company will ensure that they are under a contractual obligation to only use individual information in accordance with instructions and for no other purposes.

Subject Access Requests (SAR)

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data, as well as other supplementary information. It helps individuals to understand how and why Ranplan is using your data. An individual can make a SAR verbally or in writing, including on

social media. A request would be deemed valid if it is clear that the individual is asking for their own personal data.
Ranplan will comply with a SAR without undue delay and at the latest within one month of receiving the request (unless in complex circumstances when Ranplan may extend the time to respond by a further 2 months).

Should the copies contain supplementary information not relevant to the individual who has submitted the Subject Access Request this information will be deleted / blacked out as appropriate. If this is not possible, only data relevant to the individual will be released.

Reporting a breach in data protection

All team members, contractors and third-parties are responsible for data protection which includes a duty to report any potential breach. Should any individual be concerned that there has been a breach they should report it to the CCO. The report should include as much information as possible to enable a full investigation to take place. It is the responsibility of the COO to decide when the potential breach should be reported to the ICO.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

When a personal data breach has occurred, the COO will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is decided there is no need to report the breach a full report will be created as record of the incident.

Training

All team members, contractors and third-parties will be required to undergo training on data protection obligations. Any individual who will be handling personal data and / or sensitive personal data will undergo an additional level of training to include detailed understanding of the internal processes in place to support compliance with UK GDPR. Any individual may request a refresher of the training and should make this request to the HR Team.

Privacy Notice

Being transparent and providing accessible information to individuals about how we use their personal data is important. Ranplan has Privacy Notices on its website and on team noticeboards. In addition, there is a Data Control Log [stored on Ranplan Wireless SharePoint and Cognidox] which is owned and updated by the COO.

The Data Control Log contains information on what data is held, where it is stored, how it is used, who is responsible and any retention timeframes that may be relevant. This Data Control Log will be audited on a regular basis to manage and mitigate any risks associated with data protection.

Consent

Data that is collected is subject to active consent by the data subject. This consent can be revoked at any time unless the data that has been collected is required in order for Ranplan to exercise a legal obligation.

Criminal Record Checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject. Ranplan do not conduct criminal record checks.

Privacy by design and default

Ranplan have a general obligation to implement technical and organisational measures to show we have considered and integrated data protection into processing activities.
Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The General Manager will be responsible for conducting Privacy Impact Assessments and ensuring that all projects that involve personal / sensitive data commence with a privacy plan, for example, introducing a new customer relationship management system or a new payroll management system.

International data transfers

As a global organisation Ranplan may need to undertake an international data transfer. Should the requirement arise, the COO will be involved in any discussion where data is to be transferred to a country outside of the UK.

For reference, data is protected under The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR)

Further information is available on www.ico.org.uk.

Consequences of failing to comply with this policy

Ranplan takes compliance with this policy very seriously. Failure to comply puts individuals and Ranplan at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our Disciplinary and Grievance Policy which may result in dismissal.

Individual Consent
I hereby confirm that I have read and fully understand the terms of the Ranplan Data Protection Policy. I agree to comply with the policy, at all times, and confirm that I understand how to raise concerns about any potential breach of this policy. I understand I have the right to receive regular training and updates on data protection.

Name	
Job Title	
Date	
Signed	

[**Copy to be held on the Personal File)**