Reward Gateway Data Protection Policy

Classification – Confidential

May 2018 – Version 2.0

265 Tottenham Court Road
London
W1T 7RQ
UK

Table of contents

Document purpose

Reward Gateway is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

- 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; 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;
- 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; 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;
- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- 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.

General approach

- This policy applies to all Personal Data processed by Reward Gateway.
- The Data Protection Team shall take responsibility for Reward Gateway's ongoing compliance with this policy.
- This policy shall be reviewed at least annually.
- Reward Gateway shall register with the Information Commissioner's Office as an organisation that processes personal data.

Definitions

Term	Definition
GDPR	Means the General Data Protection Regulation.
Responsible Person	Means Will Tracz
Register of Systems	A register of all systems or contexts in which personal data is processed by Reward Gateway.
Personal Data	As defined in the GDPR.

Categories of Personal Data

Reward Gateway processes and maintains multiple independent sources of Personal Data.

For clarity, these are defined as:

Term	Definition	Business Owner
Employee Personal Data	This is personal data collected and used by Reward Gateway about it's own employees.	Group HR Director
Carer Personal Data	This is personal data that may be supplied by carer's who receive payment from RG Childcare on behalf of member's.	Group Director of Product & Client Success
Customer Personal Data	This is personal data supplied by Reward Gateway's clients for the purposes of administering the services.	Group Director of Product & Client Success
Member Personal Data	This is personal data supplied by the end-users (i.e. members of Reward Gateway's client's organisations) for the purposes of using the services.	Group Director of Product & Client Success
B2B Personal Data	This is personal data that is collected and used by Reward Gateway's Sales and Marketing teams.	Group SVP Marketing

Due to the wide ranging nature of the activities conducted by Reward Gateway in relation to this, Reward Gateway have deemed itself to be a controller (with the exception of Customer Personal Data).

Policy

Responsibilities

Reward Gateway will produce policies, procedures, guidelines and work instructions which if followed correctly will facilitate the achievement of compliance with the

requirements of the relevant legislation by individuals processing personal data in the course of their Reward Gateway duties.

This policy, and the procedures mentioned, are owned by the Data Protection Team and it is their responsibility to ensure they are kept up to date and communicated appropriately throughout the business.

Specific data handling procedures, guidelines or work instructions may also be produced by other departments, teams or line managers but if they involve the handling of personal data they must be approved by the Data Protection Team.

Responsibilities and consequences of non-compliance

Everyone who processes personal data on behalf of Reward Gateway is responsible for ensuring they comply with the requirements of this policy and the relevant legislation.

In addition line managers are required to ensure that the processing undertaken by individuals reporting to them complies with the requirements of this policy and the relevant legislation.

In the event any individual considers that the processing they are undertaking does not comply with this policy, or the relevant legislation, they should raise the issue with their line manager and the Data Protection Team.

If any individual considers that the provisions of this policy, or any of the procedures or work instructions related to it, breach the requirements of the relevant legislation they should report this immediately to the Data Protection Team.

Failure to comply with the requirements of this policy or the relevant legislation constitutes a serious breach of the applicable Code of Conduct and may result in action, which could include dismissal..

Principles relating to the processing of personal data

All processing of personal data undertaken by Reward Gateway must be in compliance with the Principles set out below. Individuals processing personal data on behalf of Reward Gateway should ensure they adhere to the Principles in addition to any specific requirements of this policy, procedures or work instructions related to it. Breach of the Principles is a breach of the GDPR. In the event of any conflict between the Principles and this policy, procedures or work instructions the Principles have precedence and the conflict should be reported to the Data Protection Team.

Under the General Data Protection Regulation there are six principles relating to the processing of personal data. They require that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

2. 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. 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 ('accuracy');
5. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
6. 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 ('integrity and confidentiality').

There are two other data protection principles set out in the Data Protection Act 1998 but have not been restated in the GDPR. These relate to the rights of data subjects and international transfers and addressed in the section below ("Rights of the Data Subject") and "Transfer of Data".

Rights of the data subject

Everyone who processes personal data on behalf of Reward Gateway must respect the privacy rights of the data subject and ensure they do not undertake any processing which breaches the rights granted under the GDPR set out below.

The GDPR grants certain rights to data subjects and Reward Gateway will issue procedures to ensure that those rights are respected and are easily exercisable by the data subjects whose personal data it is processing. The rights granted to data subjects are:

- **Right of access**
  The data subject has the right to confirmation of the processing undertaken and to a copy of the personal data being processed. This copy must be

provided free of charge and within one calendar month. Reward Gateway has detailed 'Subject Access Request Procedures' which set out how this right will be provided for.

- **Right to rectification**
  Inaccurate data must be corrected without delay and incomplete data completed upon request. Any requests to exercise this right should be forwarded to the Data Protection team without delay.

- **Right to erasure**
  Also known as the 'right to be forgotten' this provides that under certain circumstances the data subject can oblige the data controller to erase personal data relating to them without undue delay. Any requests to exercise this right should be forwarded to the Data Protection team without delay.

- **Right to restrict processing**
  Under certain circumstances the data subject can object to processing other than storage of their personal data. Any requests to exercise this right should be forwarded to the Data Protection team without delay.

- **Right to data portability**
  This entitles the data subject to a copy of their personal data in a structured and commonly-used machine readable format and allows them to require it to be transmitted to another data controller. This will most commonly apply to utility and financial services companies but Reward Gateway must be prepared to honour any such requests which should be forwarded to the Data Protection team without delay.

- **Right to object to processing**
  A data subject may object to processing including the profiling of the data subject, which is undertaken under the public interests or legitimate interests bases, and can also object to the processing of their data for direct marketing purposes (note as Reward Gateway undertakes direct marketing only with the explicit consent of the data subject and such objection will be treated as a rescinding of the consent of the data subject). Any requests to exercise this right should be forwarded without delay to the Data Protection team for actioning.

- **Right not to be subject to automated individual decision-making**
  Data subjects can object to 'automated processing' (which includes profiling) if that processing results in decisions which have a legal effect concerning him or her (or similarly significantly affects them) being made solely on the basis of that processing. At the current time no such processing is undertaken by

Reward Gateway, if any is anticipated or planned advice should be sought from the Data Protection team.

In addition to the above explicit rights the provisions of Articles 13 and 14 of the GDPR specify that certain information must be given to a data subject who is the subject of data processing at specific times, this is sometimes referred to as the 'Right to be informed' but is in fact an obligation on the data controller. The obligation is met by advising the data subject how their data will be used, for how long, the legal basis for the processing and how it will be kept secure. This information should be given when the data is collected and whenever it is to be used for a purpose which is different to the one for which it was originally collected. This will be done by reference to specific Privacy Statements provided by the Data Protection Team as part of the design of data collection forms. To ensure that sufficient notice is drawn to the Privacy Policy and the requirements of these articles are met advice should be sought from the Data Protection Team before any data collection is conducted or any personal data is used for new or novel purposes.

Record keeping

Everyone who processes personal data on behalf of Reward Gateway shall ensure that sufficient records are kept of their processing to enable the Reward Gateway to meet the requirements of the Accountability Principle as set out below. Specific work instructions may be issued to provide guidance on the records which should be kept.

In addition to the Data Protection principles set out above, Article 5 of the GDPR states that the controller shall be responsible for, and be able to demonstrate compliance with, the data protection Principles. This requires record keeping of all data processing undertaken by Reward Gateway.

The following records shall be maintained

- An Information Asset Register detailing the personal data (and category) processed, the nature of the processing, the systems used, the legal basis, the time for which the data will be retained and how it will be disposed of.
- Data Protection Impact Assessments undertaken.
- Privacy Statements and the dates and circumstances when they were used.
- Copies of the wording used to obtain consent and records of how and when consent was given by individuals to the processing of their personal data.
- A Data Breach log.
- Records of relevant training.

Personal data breaches

Everyone who processes personal data on behalf of Reward Gateway must ensure that they take all appropriate and reasonable precautions to prevent a personal data

breach occurring. In the event they become aware of such a breach they will report the matter immediately to the Data Protection Team.

Personal data breaches, except those which are unlikely to result in a risk to the rights and freedoms of the data subjects, must be notified to the Information Commissioner's Office (ICO) without undue delay and within 72 hours of the controller becoming aware of the breach.

The decision as to whether or not the breach represents a risk to the rights and freedoms of the data subject requires an in-depth knowledge of the issues involved and how personal data could be misused to create such a risk. The individual who discovers the data breach is unlikely to possess sufficient knowledge of these issues to make this judgement and therefore all personal data breaches should be reported without delay to the Data Protection Team (using the procedures outlined in the Incident Management Policy) who will assess the risks to the data subject(s) and if appropriate report the breach to the ICO.

'Near-misses' (i.e. events that could have led to a data breach if it were not for specific intervening action being taken to prevent the breach and/or circumstances which have the potential to lead to a data breach) should also be reported so that action can be taken to assess and mitigate the risk of a similar event causing a breach in the future.

Data Protection Impact Assessments

Everyone who processes personal data on behalf of Reward Gateway shall ensure that they apply 'privacy by design and default' practices by, for example, collecting only the personal data required for a specified purpose and ensuring that the data is only accessible to those who need it to carry out their Reward Gateway tasks. All projects, processes or procedures which involve the processing of personal data shall first be subject to a screening process to determine whether a Data Protection Impact Assessment (DPIA) is required. If a DPIA is deemed necessary it will be undertaken, and any identified remedial actions implemented, before personal data is processed.

The GDPR introduces the concept of 'privacy by design and default'. In essence this requires the controller to ensure that all its processing operations are designed to minimise the risk to the privacy of the data subjects. This involves measures such as data minimisation, pseudonymisation, and role based access protocols. Reward Gateway will ensure that privacy by design and default is enshrined in policies, procedures and work instructions which relate to the processing of personal data.

Processing which uses new technologies, or which because of its nature, scope, context or purposes is likely to result in a high risk to the rights and freedoms of the data subjects is, under the GDPR, subject to the requirement to carry out an assessment of the impact of the processing operations on the protection of personal data – a Data Protection Impact Assessment. Reward Gateway has Data Protection

Impact Assessment Procedures in place which must be adhered to whenever a new data processing operation which involves the collection of personal data, or the use of personal data already collected in a way which is different to that for which it was originally collected, is planned.

Transferring Personal Data outside Reward Gateway

Personal data shall only be transferred outside Reward Gateway where there is a legitimate business reason for doing so to a recipient who has been subject to due diligence checks and is bound by a contract which, by incorporation of mandatory standard clauses, specifies the purposes for which the data is transferred and restricts the use of the data to those purposes.

Reward Gateway may engage with third parties to carry out work for it which will require personal data to be transferred to that third party (e.g. sending a list of names and emails to fulfil a marketing campaign). These third parties are known as 'Data Processors'. Reward Gateway will only use Data Processors that are able to satisfy it, and provide guarantees, that they have appropriate organisational and technical measures in place to ensure the data is processed in compliance with the GDPR and who have signed a binding contract which specifies the purpose for which the personal data is transferred, restricts the processing to that purpose, specifies the duration of the contract and sets out how the data will be dealt with at the end of the contract.

The Legal team have drafted standard contract clauses to ensure the requirements of the GDPR are met when contracting with a third party to carry out data processing on behalf of Reward Gateway and these clauses must be incorporated into every contract appointing a data processor. Responsibility for incorporating these clauses and carrying out initial and ongoing due diligence checks rests with the Category managers within the Procurement team.

Overseas Transfers

Before any data is transferred overseas the Data Protection team must be notified and their approval to the transfer obtained.

If personal data is to be transferred overseas specific measures must be in place to ensure that the rights and freedoms of the data subjects are protected. Such a transfer will usually occur when contracting with a data processor, but this may not always be the case, in particular after the UK has left the European Union when transfers between Reward Gateway sites in the UK and Bulgaria may require these specific measures to be put in place.

The GDPR has three mechanisms by which overseas transfers can be safely made, an adequacy decision, appropriate safeguards or binding corporate rules. Which of these measures is appropriate depends on the nature and circumstances of the transfer and

advice should be sought from, and permission granted by, the Data Protection Team before any such transfer is undertaken.

Data Protection Training

Everyone who processes personal data on behalf of Reward Gateway, including accessing personal data, must complete the mandatory online data protection training module and demonstrate their understanding by successfully completing the accompanying test(s).

In order to ensure compliance with this policy and with the regulatory requirements relating to the processing of personal data, all individuals employed by Reward Gateway are required to complete a mandatory online data protection training module. They are also required to demonstrate their understanding of the contents of the training module and of this policy by successfully completing an online test. The training module and accompanying test should ideally be completed as soon as the individual has access to Reward Gateway systems but in any event within two months of the commencement of their employment.

Further refresher training should be undertaken at intervals dependant on the individual's role but at least once every three years.

Additional online training modules may be made available to educate individuals about specific topics covered by this policy, line managers should review these modules and the roles of individuals in their team to determine if any should be a mandatory requirement.

Legal Bases for Processing of Personal Data

All processing of personal data undertaken by Reward Gateway must be undertaken under one of the specified legal bases as set out below. The particular legal basis being used must be identified and recorded in the Information Asset Register prior to any processing being undertaken.

Under the GDPR there are six 'legal bases' for the processing of personal data. The processing of personal data is only lawful (as required by the first Principle) if one of these legal bases apply, they are:

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes ('consent');
2. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract ('contract');
3. processing is necessary for compliance with a legal obligation to which the controller is subject ('legal obligation');
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person ('vital interests');

5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller ('public interest');
6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child ('legitimate interests').

Processing Special Categories of Personal Data

The processing of Special Category personal data will only be undertaken when at least one of the exemptions as set out below from the general prohibition has been identified and recorded in the Information Asset Register.

Special category data is the description applied in the GDPR to certain types of personal data considered particularly sensitive, they are also commonly known as 'sensitive personal data'. The types of data considered to be 'special category' are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data (when used to uniquely identify an individual)
- Data concerning health
- Data concerning an individual's sex life or sexual orientation.

As a general rule the processing of special category personal data is prohibited unless one of the following conditions apply (these can be considered additional legal bases for the processing of special category data).

- The data subject has given their explicit consent 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 is necessary to protect the vital interest of the data subject or another person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of the legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim. The data should relate to members, former members or others with regular contact with the body and data should not be disclosed outside the body without specific consent.

- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Data Protection Team

In accordance with Section 4 of the GDPR, Reward Gateway is obliged to designate a Data Protection Officer or responsible person to carry out specific tasks related to ensuring compliance with the legislation on the basis that it is engaged in regular and systematic monitoring of data subjects on a large-scale.

Rather than a single individual, Reward Gateway have opted to delegate this function across the following areas:

Role	Responsibilities
Chief Technical Architect	• Overall governance framework.
Head of Information Security	• Training. • Handling of data subjects rights. • Maintenance of the Information Asset Register.
Information Security Auditor	• Auditing and enforcing of policies.

The responsible person has a direct reporting line to the Chief Executive but day to day line management of the responsible person may be allocated to another person.

This decision will be reviewed annually to take into account new guidance which may be issued by the Information Commissioner's Office.

Relationship with Information Security Management System

In the event of a conflict between the requirements of the Information Security Management System and this Data Protection Policy which relates to the processing of personal data, the provisions of this Policy shall have precedence.

Effectiveness

The business needs to be assured that this policy is working i.e.

1. It is doing what it is supposed to do on the ground
2. It is effective at delivering the organisational objectives.

This will be achieved this by having:

- A Data Protection Team to oversee the policy.
- A Data Governance Authority in place to oversee the management and compliance of Reward Gateway with the Policy.

- Regular audits carried out and reports issued by the Data Governance Working Group to assess compliance with policy.

Review

Reviews of this policy will take place at least once a year. However additional reviews may be triggered by any of the following items assessed by the Data Protection Team:

- Escalation of related strategic risks
- Significant ethical changes
- Regulatory changes, in particular the coming into force of the GDPR/UK Data Protection Bill/The E-Privacy Regulation
- Guidance issued by the ICO which significantly impacts this Policy
- External or internal incidents (e.g. data breach, negative publicity)
- New technology
- Financial changes
- Changes to governance

Revision history

Rev	Date	Author	Description	Approved	Date
2.0	15.05.2018	Will Tracz	New draft under GDPR.	Doug Butler	28.05.2018