Data Protection Policy

Version Control

Note: minor updates increase version number by 0.1; major updates increase version number by 1.0.

Version Number	Sections Amended	Date of update	Approved by	Date of approval
1.0	First version		GCBD	September 2019
1.1	Various to amend page numbers and job titles	18.11.19		

Document owner: Company Secretary

Review date: 30 September 2020

Table of Contents

1 Policy statement

Radian Group refers to, Radian Group Limited, the parent company and all of its subsidiary companies which, for the avoidance of doubt includes Yarlington Housing Group and its subsidiaries.

1.1 Radian Group regards the fair correct and lawful treatment of personal data to be essential to the success of its business and to maintaining the trust of customers, colleagues, contractors, suppliers and other stakeholders.

1.2 Radian Group's Data Protection Policy (**this Policy**) sets out our commitment to protecting the personal data which we process in carrying out our business and providing the services which our customers need and expect from us. It sets out how we implement that commitment with regards to the collection and use of personal data and aims to ensure that we will:

1.2.1 comply with applicable data protection law and follow good practice;

1.2.2 protect the rights and freedoms of those whose personal data we use;

1.2.3 be open and transparent in the way we collect, use, share, store and delete personal data; and

1.2.4 have appropriate technical and organisational safeguards in place to minimise the risk of a data breach.

1.3 This Policy applies to all individuals who process personal data on behalf of Radian Group including but not limited to staff, involved customers, contractors and board members of Radian Group itself and any of its affiliated companies.

1.4 Those using or accessing personal data on behalf of Radian Group are required to be familiar and comply with this Policy.

1.5 This Policy does not form part of any employee's contract of employment and may be amended at any time.

1.6 The Data Protection Officer (DPO) for the Radian Group is Gemma Burton-Connolly, Company Secretary.

2 Data protection legal framework

2.1 We are committed to ensuring that we comply with the requirements of the data protection laws in force in England and Wales (**the Data Protection Laws**). The Data Protection Laws include the General Data Protection Regulation (**GDPR**) and the Data Protection Act 2018 as they are in force from time to time. The Data Protection Laws also include any formal written guidance published by the Information Commissioner's Office (**ICO**).

2.2 The Data Protection Laws apply to personal data which is defined as any information from which a living individual can, or potentially can, be identified, from this information or when combined with other information (for example a name, identification number, location data, an online identifier or factors specific to the physical, mental, economic, cultural or social identity of a person). Certain types of personal data are deemed special category (also known as 'sensitive personal data') and are given additional protection under the Data Protection Laws. These special categories cover information regarding:

- Race or ethnic origin,
- Political opinions,
- Religious beliefs,
- Trade union membership,
- Physical or mental health and biometric data; and
- Sexuality and gender.

2.3 The Data Protection Laws apply to information about individuals which is in digital form or in hard copy. Organisations that decide how and why personal data is processed are known as '**Data Controllers**'. Radian Group, is a Data Controller, as are those of its affiliates. References to Radian Group in this Policy shall be understood to include any of these affiliates which also act as Data Controllers.

2.4 Contractors that process personal data on behalf of Radian Group as part of a service are known as '**Data Processors**'. Whenever a contractor acts a Data Processor for Radian Group an agreement shall be put in place between Radian Group and the contractor which meets the requirements of Article 28 GDPR and adheres to the Data Processor Procedure.

3. Data protection principles

3.1 The data protection principles of GDPR form the bedrock of the Data Protection Laws and must be complied with at all times when personal data is processed. The data protection principles require that personal data is:

3.1.1 used in a way which is lawful, fair and transparent (***the first data protection principle***);

3.1.2 only collected for a specified, explicit and legitimate purpose (***the second data protection principle***);

3.1.3 adequate, relevant and limited to what is necessary for processing purpose (***the third data protection principle***);

3.1.4 accurate and up to date (***the fourth data protection principle***);

3.1.5 kept in a form which allows identification of individuals for no longer than necessary (***the fifth data protection principle***); and

3.1.6 kept appropriately safe against unauthorised processing, accidental loss, destruction or damage (***the sixth data protection principle***).

4. Lawful conditions for processing

4.1 The first data protection principle requires us to ensure that we have a lawful basis for any processing of personal data. There are six lawful bases prescribed in Article 6 of the GDPR namely:

4.1.2 the individual has provided their consent for the use of their data for a particular purpose;

4.1.3 the use of an individual's personal data is necessary for the performance of a contract with the individual;

4.1.4 the processing is necessary for compliance with a legal obligation imposed on the Data Controller;

4.1.5 the processing is necessary in order to protect the vital interests of the individual or another;

4.1.6 the processing is necessary for the performance of a task in the public interest; and

4.1.7 processing is necessary for the purposes of the legitimate interests of the Data Controller, except where these interests are overridden by the interests or rights of the individual.

4.2 We shall only process personal data if we can rely on one of the lawful bases, and/or another set out in the Data Protection Act 2018. If the processing involves special category personal data we shall also rely on one of the additional lawful bases required under Article 9 GDPR, which in most circumstances will be the explicit consent of the individual. Guidance on selection of an appropriate lawful basis is set out in Radian Group's Lawful Processing Guide.

4.3 The lawful basis on which we shall rely in relation to any particular categories of personal data and special categories of personal data shall be documented on our Information Asset & Risk Register (**IAAR**).

4.4 We shall inform individuals of the lawful basis on which we shall rely when processing their personal data through the means of a Privacy Notice which has been made available to them.

5. Consent

5.1 Where consent is the lawful basis for processing personal data, the consent must be freely given by the individual. If there is an imbalance of power between us and the individual, consent can rarely be said to be freely given. Typically, there is an imbalance of power between an employer and employee. In most cases making the provision of an individual's consent a condition for us to provide a service to that individual will call into question whether the consent was given freely, so in those cases we should avoid the use of consent if possible.

5.2 Consent must also be specific. We need to be clear about what we are seeking consent for and the request should not exceed what is necessary for meeting the specified business purpose. The individual must also take an active step to indicate that they are providing their consent; silence, pre-ticked boxes or inactivity do not constitute consent.

5.3 Consent must be recorded in writing and stored in digital or hard copy format

5.4 Consent can be withdrawn at any time, and the method of doing so should be clearly explained both on the consent form and in the appropriate Privacy Notice. Once consent has been withdrawn we cannot seek to rely on another lawful basis to continue processing the same kind of personal data for the individual who has withdrawn their consent.

6. Individual's rights

6.1 The Data Protection Laws provide individuals with prescribed rights relating to the use of their personal data. We will respect those rights, treat the individual making the request with courtesy and endeavour to meet the request on time and in full where possible. The processes we will follow in fulfilling these rights' requests are set out in:

6.1.1 the Subject Access Request Procedure, where an individual makes a right of access to personal data request under Article 15 GDPR: or

6.1.2 the Data Subject Rights Procedure, where an individual makes a rights request:

(b) for rectification of personal data, under Article 16 GDPR;

(c) for erasure of personal data, under Article 17 GDPR;

(d) for restriction of processing personal data, under Article 18 GDPR;

(e) for portability of personal data, under Article 20 GDPR;

(f) to object to processing of personal data, under Article 21 GDPR; and/or

(g) not to be subject to automated decision making, under Article 22 GDPR.

6.2 All rights requests must be notified to the Data Protection Officer (**DPO**) as soon as possible and records of their fulfilment will be kept in a Register maintained by the DPO.

6.3 Any individual who is not satisfied with our response to their rights' request will be invited to discuss the matter with us and informed of their right to lodge a complaint with the ICO.

7. Transparency

7.1 The first data protection principle requires us to be transparent in relation to the personal data which we use. Radian Group will be open about the types of personal data we process, how the personal data may be processed by us or by our Data Processors, our purpose in doing so, with whom the personal data might be shared, the period it will be kept for, whether it will be stored within the European Economic Area or elsewhere, and our lawful basis for each kind of processing we undertake. This information will be made easily accessible through the provision of Privacy Notices.

7.2 We have a suite of Privacy Notices relevant to the categories of individual or subject matter that they address.

7.3 All Privacy Notices will be published on Radian Group's website and made available to individuals at the point of collection of personal data and, where appropriate, through the customer portal. They are reviewed regularly to ensure their accuracy and relevance to the category of individuals which they address.

8. Accountability and data management

8.1 Data protection by design and default

8.1.1 Data Protection Laws require us to consider data protection by design and default. This obligation requires us to consider the data protection implications of any project or process both at the point of inception and throughout the life of any processing. Data protection is something which should also be a consideration in relation to everything and anything we do with personal data.

8.1.2 Those who use personal data on our behalf are required to consider data protection by design and default.

8.2 Record keeping

8.2.1 Data Protection Laws require us to maintain records of our data processing activities. Those records shall be created, maintained and held by our DPO in the IAAR. The IAAR will be made available for inspection by the ICO upon request.

8.3 Data Protection Impact Assessment

8.3.1 A Data Protection Impact Assessment (**DPIA**) is an essential tool for demonstrating our compliance with Data Protection Laws. It is used to work out the impact which our use of personal data will have on individuals, particularly where new technology or innovative methodology is involved, and is required by law if our use of personal data is likely to result in a high risk to individuals. Where this is the case a DPIA should be completed before a new project or operation involving personal data begins. Our approach to DPIAs is set out in the Data Protection Impact Assessment Procedure and Toolkit.

9. Sharing and transferring data

9.1 Before sharing personal data with any third party we must be sure that we have a lawful basis for doing so. Privacy Notices will contain information about the organisations with which we are likely to share personal data and give our lawful basis for doing so.

9.2 For some kinds of data sharing, a consent from the individual is needed before disclosure occurs. This is the case for sharing information with Customer's Authorised Contacts and our approach to this is set out in the Authorised Contact Procedure/Authority to Discuss Procedure. In other cases consent may not be the lawful basis for sharing information and we may even disclosure information without giving prior notice to the individual concerned, for instance where we are asked by the police to disclose information to support the prevention or detection of crime, or where a serious safeguarding issue has arisen and we are asked by Social Services to disclose information that will support their safeguarding role. Under such circumstances, staff will ensure the request is legitimate, and seek guidance from the DPO, before the disclosure takes place.

9.3 Where we share personal data with a third party organisation, either regularly or for a one off project, we shall consider whether a data sharing agreement and/or non-disclosure agreement is appropriate in the circumstances. Advice should be taken from the DPO before a decision is made. If a data sharing agreement is completed, this will be recorded on the IAAR.

9.4 Compliance with Data Protection Laws will be a standard requirement for any data sharing agreement or non-disclosure agreement. Any personal data involved will be

shared through an appropriately secure method, e.g. encrypted email or secure portal.

9.5 Radian Group shall not transfer, nor permit those with whom it shares personal data, to transfer any personal data outside of the European Economic Area unless our DPO has confirmed that such a data transfer is lawful and appropriate in the circumstances.

10. Data risks, breaches and security

10.1 A data breach occurs when personal data is lost, disclosed to or, accessed by those who have no authority to see it or use it, or when it is made unavailable for use (for example by ransomware) or corrupted and made unreliable (for example by malware), whether or not the individual(s) whose personal data is affected has any knowledge of what has occurred or is directly harmed by the breach.

10.2 In applying this Policy and associated procedures Radian Group aims to ensure that it is taking all reasonable measures to protect Radian Group and the individuals whose personal data it processes, from the serious risks associated with data breach, including: loss of confidentiality, reputational damage, loss of trust and financial loss. Every incident that represents a data breach or a 'near miss' data breach is taken very seriously by Radian Group.

10.3 As part of our commitment to high data security standards, and robust and effective risk management, Radian Group will:

10.3.1 obtain and maintain Cyber Essentials accreditation to help limit the risk in relation to cyber-related data breaches;

10.3.2 ensure that all colleagues who work with personal data are properly trained in the processing of personal data, in accordance with Radian Group policy, procedures and best practice standards, and are aware of their own permitted access levels, as well as the data risks associated with their particular roles, and how to mitigate these;

10.3.3 promote a culture of awareness and respect for data privacy rights at all levels across its business; and

10.3.4 where reasonable and proportionate to the circumstances, take action, including staff disciplinary action and the termination of agreements with Contractors, where it appears that relevant policies and procedures are not being properly applied.

10.4 Anyone who is using personal data on Radian Group's behalf (whether staff or Contractor) is required to report all actual suspected or near-miss data protection compliance failures and breaches ('**data incidents**') to the DPO as soon as they are discovered. The Data Breach Procedure sets out in detail the steps to be taken and

the roles and responsibilities of all those involved in the processing of personal data at the time such a data incident occurs.

10.5 The DPO shall maintain a data breach register in order to monitor themes and trends in data incidents, and record lessons learned. The DPO will also ensure that:

10.5.1 the Information Security Forum (ISF) is regularly informed about data incidents occurring since the previous meeting of the ISF;

10.5.2 any data breach which is determined (after discussion by the ISF) to be notifiable to the ICO shall be notified in writing to the ICO within 72 hours of the data breach being reported to or discovered by any member of Radian Group staff.

11. Monitoring and compliance

Data Protection Audits will take place in line with Data Protection Law requirements at regular intervals, but no less than once every three years, unless the ISF determines that due to the number and/or severity of breach incidents over a six month period, an audit should occur sooner.

12. Roles and responsibilities

Information Security Forum

12.1 In order to ensure good information governance, the ISF has been established to provide ongoing steer, support, and monitoring of best practice and compliance with Data Protection Laws, as well as targeted advice to senior management in respect of:

12.1.1 general levels of Data Protection Law compliance within Radian Group;

12.1.2 any instances of serious non-compliance with the Data Protection Laws, established through audit, whistle-blowing or a series of data incidents;

12.1.3 responses to any particular serious data breach including mitigation steps, crisis management strategies, notification of ICO and any subsequent liaison with ICO;

12.1.4 meeting individuals' rights requests under the Data Protection Laws and monitoring the handling of individuals' complaints to the ICO;

12.1.5 the maintenance of the IAAR; and

12.1.6 overseeing the conduct of DPIAs and providing input and approval to high risk DPIA requests.

12.2 The ISF membership consists of the following posts:

12.2.1 Senior information risk owner (SIRO); Executive Director of Strategy, Business Intelligence and HR

12.2.2 Company Secretary and Data Protection Officer

12.2.3 Head of Business Assurance

12.2.4 Director of IT and Innovation

12.2.5 Head of Operations & Customer Experience

12.2.6 Data Protection Adviser

12.2.7 Head of Legal and Compliance.

12.3 Other individuals may be temporary members of the Group at certain times as required.

Data owners (Information Asset Owners)

12.4 These are the heads of service or senior managers who are responsible for ensuring that specific personal information assets are accounted for, managed processed and retained appropriately and in accordance with this Policy, and the procedures which relate to them. Their key responsibilities are to:

12.4.1 lead and foster a culture that values and protects the responsible and lawful use of personal data;

12.4.2 know what information assets they are responsible for, why they are collected, how they are used, and for what purpose;

12.4.3 determine whether and with whom any information asset may be shared, and ensure that sharing is justified under the Data Protection Laws (after consultation with the DPO, where necessary) and supported by a data sharing agreement (if advised by the DPO);

12.4.4 be responsible for defining who should have access to the information asset within Radian Group, why the access is needed, and, in cases of highly sensitive information, ensure that use of the information asset is periodically monitored;

12.4.5 identify any risks to the information asset, and support risk management activity directed at the integrity, availability, minimisation and confidentiality of the information asset; and

12.4.6 ensure that any project which has the potential to impact individuals' data privacy rights has been reviewed to determine if a DPIA should be carried out, and if so that the DPIA is carried out.

Other responsibilities

12.5. The Board and Executive Team are responsible for establishing and maintaining a control environment that promotes overall compliance as well as approval of this policy and any significant amendments or updates made to it.

12.6 All staff, involved customers, and Board Members are responsible for ensuring, whilst undertaking their roles that they do so in compliance with this Policy and the Data Protection Laws. They also have responsibility to report data incidents to the DPO.

12.7. The DPO will be responsible for:

12.7.1 completion of tasks set out in Articles 38 and 39 of the GDPR and ensuring that Radian Group remains compliant with this Policy and Data Protection Laws.

12.7.2 maintaining Radian Group's registration with the ICO and for handling data protection questions from staff and all those covered or affected by this Policy; and

12.7.3 providing guidance on interpretation and application of Data Protection Laws, and

12.7.4 review and update of this Policy and the rest of the Data Governance Framework (as set out below).

12.8 The Director of IT and Innovation is responsible for:

12.8.1 ensuring that all systems, services and equipment used for storing and management of data meet security standards agreed as acceptable by the ISF;

12.8.2 performing regular checks through scans and penetration testing etc. to ensure security hardware and software is functioning properly; and

12.8.3 evaluating the security of any third party services the company is considering using to store or process data.

12.9 The HR and Learning & Development Team, along with the DPO and Data Protection Adviser, are responsible for the provision of adequate training for staff.

12.10 The Procurement Manager is responsible for ensuring that all contracts and tender documents are compliant with Data Protection Laws and that the Contractor has adequate policy and procedures in place to achieve compliance.

12.11 The Director of Communications is responsible, in liaison with the DPO and Data Protection Adviser for:

12.11.1 addressing any data protection queries from journalists or media outlets;

12.11.2 ensuring that publications to customers and stakeholders abide by this Policy and Data Protection Laws.

13. Data Governance Framework and associated policies

13.1 This Policy is the overarching document for Radian Group's Data Governance Framework. Other documents which form part of this framework are:

13.1.1 The Subject Access Request Procedure;

13.1.2 The Information Asset and Risk Register;

13.1.3 The Data Processor Procedure

13.1.4 The Lawful Processing Guide

13.1.5 The Data Security Procedure

13.1.6 The Data Breach Procedure

13.1.7 The Authorised Contact Procedure/Authority to Discuss Procedure

13.1.8 Data Breach Register

13.1.9 The Data Protection Impact Assessment Procedure and Toolkit

13.1.10 The Data Subjects Rights Procedure

13.1.11 Document Retention Policy

13.2 Other Policies and Procedures to consider which that should be read in conjunction with this Policy are:

13.2.1 Social Media Policy

13.2.2 Secure Encryption Policy

13.2.3 ICT Systems usage Policy

13.2.4 IT – Agreeing Access Rights & Changes Procedure

14. Policy review

This policy will be reviewed every two years or following any changes or updates in relevant legislation