Radian Group Inc. Data Privacy Compliance Policy

1. Overview

a. This Data Privacy Compliance Policy ("Policy") of Radian Group Inc. and its wholly owned subsidiaries and affiliates (collectively, "Radian" or the "Company"), establishes the standards and guidelines for compliance with the various laws in the United States and other jurisdictions, as may be applicable, regarding the permissible use and protection of private and personal information of Radian directors, employees, contractors, customers, consumers and other natural persons which is provided to, or held, controlled or processed by, the Company.

b. In the course of its business, Radian regularly obtains and uses certain information about consumers, customers, vendors, business contacts, directors, employees, contractors and others, which from time to time may include personal and private information. This Policy describes how private and personal data must be handled or stored to meet the Company's privacy requirements and standards, and to comply with applicable laws in a manner that supports and complements Radian's strategic objectives and the Radian Code of Conduct and Ethics ("Code").

c. Radian's handling of personal data is also governed by one or more data protection and cybersecurity laws that govern how personal, private, confidential or sensitive information is protected from data breaches. It is imperative that everyone working for or on behalf of Radian understands and complies with the obligations and standards set forth in applicable data protection and cybersecurity laws, as reflected in the guidelines set forth in the Code, the Acceptable Use Policy and related Information Security policies.

2. Scope

This Policy represents our shared responsibility to properly handle private data and applies to everyone who acts on behalf of Radian (collectively, "Personnel"). This includes:

All regular full-time and part-time employees, regardless of their business unit or subsidiary;

All Radian temporary, contract, and contingent workers; and

Members of Radian's Board of Directors.

Any person or entity to whom Radian provides personal or confidential information.

3. Purpose of the Policy: This Policy is intended to achieve the following:

a. The primary purpose of this Policy is to ensure compliance with all applicable Data Privacy Laws, consistent with the products and services being provided by Radian and where Radian conducts business operations.

b. A related purpose of this Policy is to reinforce compliance with the Code and related Company policies.

c. This Policy is intended to ensure that Radian:

i. Complies with applicable privacy laws and follows good business practices with respect to data protection, use, handling, and storage;

ii. Protects the rights of its Personnel;

iii. Is as transparent as is reasonably required to appropriately store, use and process data from Data Subjects;

iv. Is reasonably protected from the risk of a data breach of personal data, in accordance with the Code;

v. In the event of a data incident or breach, complies with applicable data security and privacy laws.

4. Definitions

a. "Data Privacy Laws" means, collectively, all applicable data privacy and protection laws which govern how Radian should collect, handle, process, use, share, transfer, store, dispose of and protect Personal Data.

b. "Data Subject" means a natural person; someone who can be identified or is identifiable, directly or indirectly, by reference to an identifier such as a name, identification number, location data, or other such similar information.

c. "Personal Data" means information which can reasonably be identified with respect to a Data Subject, and which is deemed personal or private under applicable law. Examples may include, singularly or in combination with other information: unique personal identifiers such as person's name social security number; driver's license number; account name, number, balance, transaction and/or payment history; consumer account history; credit history or credit score; passport number; postal address; internet

protocol address; personal email address; personal telephone number; date of birth; gender; account numbers; insurance information; health and medical information; disability information; tax identification information; salary and benefits information; leave periods or basis for leave; equal opportunity monitoring information; information provided by or collected about a consumer to obtain or provide a financial product or service; and consumer financial transaction information; or information from a consumer credit report.

5. Implementation

a. Responsibility for the implementation and continued management and support of this Policy is as follows:

i. The Chief Legal Compliance Officer is responsible for overseeing the legal compliance aspects of the Policy, including (a) advising on the design and establishment of a framework for compliance with the legal, regulatory and business conduct obligations outlined in the Policy; (b) identifying privacy related legal risk and providing legal support for the Company's information security, data governance, physical security, records management, human resources and other Radian business units responsible for the operational aspects of privacy and data protection compliance; (c) establishing a process to ensure that agreements entered into by the Company address the requirements defined in this Policy, as may be appropriate; (e) communicating the requirements of this Policy to third parties as may be applicable; (f) providing legal support and oversight for the functional areas which process Access Requests (as defined herein); (g) supporting Radian's efforts to train those working for Radian and who handle Personal Data regarding the requirements of this Policy; (h) overseeing all legal aspects of privacy compliance in coordination with Radian's Enterprise Compliance Office.

ii. The Chief Information Security Officer is responsible for developing policies and best practices for prevention of data breaches and other cybersecurity events, including implementation of controls and processes for security planning, incident management, improvement and reporting, pursuant to applicable Information Security policies.

iii. The Chief People Officer is responsible for identifying and taking reasonable steps to safeguard employment related Personal Data and ensuring that employee and applicant related personal data is used, stored and handled in compliance with applicable Data

Privacy Law and for supporting and enforcing compliance with the Policy.

iv. The head of Enterprise Risk Management is responsible for tracking and reporting on risks to Radian which may arise under applicable Data Privacy Laws and ensuring that the requirements of this Policy are aligned with Radian's Enterprise Compliance, Data Governance and Records Governance programs.

v. The head of Administration is responsible for maintaining the physical security of Radian's facilities in a manner that is designed to protect the confidentiality of Personal Data.

vi. Managers are responsible for ensuring that their direct reports comply with the requirements of this Policy.

6. Compliance with Applicable Data Privacy Laws

a. Personal Data of Data Subjects may be protected by one or more Data Privacy Laws, which often apply regardless of whether data is stored electronically, on paper, or on other materials or media. Radian collects, maintains, shares and otherwise processes Personal Data, including Personal Data supplied by Radian customers. This information is protected from improper disclosure under the Gramm Leach Bliley Act (GLBA) and implementing regulations. Depending on the type of data and relevant circumstances, Radian may also be subject to state privacy laws, including but not limited to the California Consumer Privacy Act (CCPA), as well as other Data Privacy Laws.

b. As may be applicable to comply with Data Privacy Laws, Personal Data must be (I) collected and used lawfully; (ii) collected only for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes; (iii) adequate, relevant and limited to what is necessary in relation to the legitimate purpose for which it is being held; (iv) accurate and, where necessary, kept up to date; (v) 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; (vi) processed and stored safely to avoid any breach of the security of Personal Data in Radian's possession or control.

c. Compliance with this Policy, the Code, all related company policies and Radian's privacy practices is of the highest importance to Radian. Personnel are required to comply with applicable Data Privacy Laws, as set forth in the Code, the Acceptable Use Policy and in related Information Security policies. Radian's data privacy practices are set forth

in its online privacy policy (https://radian.com/privacy-policy) and its Notice of Insurance Information Practices (https://radian.com/notice-of-insurance-information-practices).

d. When working with Personal Data, such as social security numbers, dates of birth, credit scores and personal financial information, protect it and use it correctly. Follow these guidelines when using Personal Data that belongs to consumers or other persons:

   i. Make sure that you are authorized to access or handle the Personal Data and that you understand the permitted purpose for which you are using it.

   ii. Collect or handle Personal

   iii. Data only for an approved business purpose and use it only for the purpose for which it was collected or provided.

   iv. Protect Personal Data from unauthorized access, loss or misuse, including not sharing it with unauthorized third parties, keeping a clean and secure workspace in accordance with the Clean Desk Policy, avoiding discussions of Personal Data or leaving sensitive documents in view in shared or public spaces.

   v. Personal Data can only stay private if it is kept secure. Safeguard access to systems which contain Personal Data, in according with the Code, Acceptable Use Policy and other Information Security policies. Use of Radian's network and communications platforms is discretionary and may be revoked or modified at any time.

   vi. Follow all applicable laws, regulations and policies related to collecting, protecting and using it, including data privacy and security laws.

   vii. Hold any third parties to whom we provide Personal Data to these standards.

e. If you have any questions about access to or handling of Personal Data, suspect a misuse of Personal Data or to report a suspected violation of the Data Privacy Laws, company policy or the Code, contact your manager or the Head of Compliance.

f. Violation of Data Privacy Laws may result in the imposition of severe fines, reputational harm, impediments to conducting or loss of business and claims by private individuals. Accordingly, noncompliance by Radian

Personnel may result in action by the Company, including up to and including termination of employment for employees.

7. Process (Law Enforcement or Legal Process) Access Requests

a. In certain circumstances, Data Privacy Laws allow Personal Data to be disclosed to law enforcement agencies without the consent of the Data Subject. If such a disclosure is requested, it is called a "Process Access Request." In response to a Process Access Request, Radian may be subject to response deadlines. Under these circumstances, Radian may disclose such Personal Data which is subject to these requests. Radian will endeavor to respond, as appropriate, within restricted time periods after (a) verifying the legitimacy of the Process Access Request, and (b) reviewing the request in consideration of any other applicable regulations and laws of the relevant jurisdiction.

b. Personnel receiving a Process Access Request from a third party are not authorized or permitted to directly respond to such requests. All responses to Process Access Requests shall be reported to the Chief Legal Compliance Officer and will be handled by the Radian Legal Department.

c. Personnel are instructed to ***immediately*** provide the Process Access Request, and any and all relevant information relating to the Process Access Request, to the Chief Legal Compliance Officer for review and handling and are required to implement instructions given by the Company in this respect.

8. Privacy of Employment Related Data

a. Radian's goal is to ensure that Radian Personnel, former employees, job applicants or those who otherwise share employment related personal information with Radian are aware that their Personal Data is being held and processed, and that they understand, as applicable and required by law:

i. That they may have a right to access, rectify or suppress their Personal Data, limit or object to the processing of, or withdraw their consent to, the portability of their Personal Data as well as to file a complaint before a competent authority;

ii. The nature of the Personal Data that the Company holds about them and why;

iii. How and why their Personal Data is being processed and maintained;

iv. How their Personal Data may be transferred, to whom and where;

v. How the Company is meeting its data protection obligations with respect to their Personal Data.

b. Radian maintains personnel records on each of its employees. The personnel file may include information such as the employee's job application, resume, performance appraisals, salary increases/compensation adjustments, background screening information and other employment related records. Training files containing educational degrees and/or certifications as well as internal and external records of training are also maintained (separately) by the Human Resources Department.

c. Personnel and training files are the property of Radian. Access to or the copying or dissemination of the information they contain is restricted to certain key Human Resources personnel and other authorized individuals. Upon request, Personnel are eligible to inspect records in their personnel files in accordance with Human Resources policies and, where applicable and as may be required by law, to access, rectify or remove their Personal Data, limit processing or object thereto, limit data portability, withdraw their consent and file a complaint before an applicable tribunal, agency or supervisory authority. If they wish to do so or have more information about the processing of their Personal Data, they must make a request of their human resources People Business Partner, or Radian's Chief People Officer. At that time, they will be informed of the procedure and conditions governing personnel record inspections and how to exercise any applicable rights with respect to their employment related Personal Data.

9. Data Retention

a. Personal Data must be maintained in compliance with its Records Management Policy and Enterprise Records Retention Schedule**.** Retention periods are intended to address:

i. Any legal obligations under applicable law to retain Personal Data for a certain period (for example in relation to regulated industries, tax, health and safety and employment laws);

ii. Radian's ability to conduct business and provide services to its customers;

iii. The statute of limitations under applicable law(s);

iv. Radian's obligation to address any disputes or potential disputes; and

v. Guidelines issued by any relevant regulatory authorities.

b. Radian's policy is to dispose of Personal Data which it no longer needs and is no longer required to maintain to comply with its legal obligations or for permissible business purposes. Where necessary or appropriate, Radian anonymizes, deidentifies and/or aggregates information to protect the Personal Data of Data Subjects, and so that Data Subjects cannot be identified by or from the anonymized data in any way.

10. Review of Policy

a. This Policy is reviewed on an annual basis and revised to reflect changes in the law and Radian's business practices.

11. Communication of Policy

a. The Policy should be communicated to key stakeholders through education, training and other means, as may be appropriate.

12. REVISION HISTORY:

Version Date:	Revision:	Author:
07/6/2020	Implementation - original written Policy finalized	Radian Legal
12/21/2020	Update review – no changes	Radian Legal
1/4/2023	Changed name to distinguish from public facing online privacy policy; formatting changes; updated language and responsibilities to align to features of Radian's Enterprise Compliance program; updated to reflect changes in state privacy law.	Radian Legal
11/25/2024	Updated references to Records Management Policy and Enterprise Records Management Schedule.	Radian Legal