

## VW CREDIT, INC.

### VW CREDIT, INC. PRIVACY REQUIREMENTS POLICY

This VW Credit, Inc. Privacy Requirements Policy (“**Policy**”) applies if a third party (“**Supplier**”) is providing services, products, or materials to VW Credit, Inc. (“**VCI**”) and will Process Personal Information in connection with the agreement between VCI and Supplier (the “**Agreement**”). This Policy contains specific requirements relating to VCI Personal Information that Supplier, its personnel, and any of its affiliates or subcontractors may access in its performance of the Agreement. This Policy is incorporated by reference into the Agreement. This Policy applies only to the Personal Information or Deidentified Data of VCI and is not meant to impose any right or obligation on Supplier in the processing of Supplier’s own Personal Information or Deidentified Data, or the Personal Information or Deidentified Data of Supplier’s other clients.

#### 1. **Definitions.**

1.1 “**Deidentified Data**” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a specific particular natural person.

1.2 “**Personal Information**” means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular natural person.

1.3 “**Privacy Laws**” means any Applicable Laws relating to data privacy and data protection, including any applicable implementing regulations, as may be in force and amended from time to time, including, but not limited to: (i) the Federal “Privacy of Consumer Financial Information” Regulation (12 CFR Part 30), as amended from time to time, issued pursuant to Section 504 of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. §6801, et. seq.) (the “**GLBA**”); (ii) the Federal Fair Credit Reporting Act 15 U.S.C. §§1681 et. seq. (the “**FCRA**”), (iii) California Consumer Privacy Act (Ca. Civ. Code 1798.100 et seq.), as amended by the California Privacy Rights Act (the “**CPRA**”); (iv) New York 23 NYCRR §500; and (v) all other applicable federal, state or local laws, statutes, rules, codes, directives, regulations and ordinances relating to the privacy and security of Personal Information, consumer protection, or security breach notification. For the avoidance of doubt, the laws included in the definition of Privacy Laws are not exhaustive and any law not listed is not excluded from the Agreement if applicable under the definition of Privacy Laws.

1.4 “**Process**”, “**Processing**” or “**Processed**” means the collecting, accessing, displaying, viewing, obtaining, creating, generating, managing, modifying, transporting, transmitting, storing, destroying, or any other handling of Personal Information in any medium (electronic or physical).

**VW CREDIT, INC.**

**2. Privacy Requirements.**

2.1 Supplier will implement and maintain a written privacy program to ensure Personal Information is only Processed in compliance with applicable Privacy Laws and as permitted under the Agreement (“**Privacy Program**”). When requested, Supplier must provide VCI with a copy of the current Privacy Program. The Privacy Program must ensure that:

- each person Processing Personal Information received from, or on behalf of, VCI is subject to a duty of confidentiality with respect to the data;
- the sale of Personal Information received from, or on behalf of, VCI is prohibited;
- the sharing of Personal Information received from, or on behalf of, VCI for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, is prohibited;
- the Processing of Personal Information received from, or on behalf of, VCI is prohibited except as necessary for the performance of the Agreement by Supplier or for the specific business purposes permitted under the Agreement;
- the Processing of Personal Information received from, or on behalf of, VCI is prohibited for any commercial purpose as defined by the CPRA other than the business purposes specified in the Agreement, including in the servicing of a different business, unless expressly permitted by the CPRA or its regulations;
- any VCI Data Handling Subcontractors (as defined in the VW Credit, Inc. Vendor Risk Management Policy) are required to engage in a written contract requiring the Subcontractor to follow this Privacy Requirements Policy;
- Supplier will cooperate with VCI in responding to any consumer rights request granted by Privacy Laws, including by:
  - implementing processes to identify what Personal Information is held on a specific individual, for what purposes such Personal Information was collected, and with whom such Personal Information was shared and why;
  - implementing processes to prevent disclosure of Personal Information of a specific individual who has opted out of data selling or sharing;
  - forwarding any consumer rights request received by a VCI customer to VCI within three days of receipt;
  - cooperating with requests by VCI to comply with consumer rights requests, including requests to delete Personal Information, within five days of receiving such request from VCI; and
  - notifying any VCI Data Handling Subcontractors who may have accessed such Personal Information through the Supplier to delete the consumer’s Personal Information unless this proves impossible or involves disproportionate effort;

2.2 Supplier shall notify VCI no later than five (5) business days after if makes a determination that it can no longer meet its obligations under Privacy Laws. In the event that VCI

## VW CREDIT, INC.

identifies any problem(s) with the Privacy Program or any proposed changes, Supplier will, at Supplier's expense:

- prepare and provide VCI with a plan to correct such problem(s) within thirty (30) days from VCI's identification of the problem(s);
- implement and complete the plan, as mutually agreed upon by the parties, within ninety (90) days from VCI's identification of the problem(s); and
- keep VCI updated with status reports during the implementation of the plan.

Following the correction of such problem(s) by Supplier in accordance with the plan, Supplier will provide VCI with a revised copy of the Privacy Program. The Supplier will allow, and cooperate with, reasonable assessments by VCI or VCI's designated assessor; alternatively, Supplier may arrange for a qualified and independent assessor to conduct an assessment of Supplier's policies and technical and organizational measures in support of the obligations under this Privacy Requirements Policy using an appropriate and accepted control standard or framework and assessment procedure for such assessments. Supplier shall provide a report of such assessment to VCI upon request.

**3. Deidentified Data Requirements.** If the performance of the Agreement by Supplier involves Deidentified Data, Supplier will:

- take reasonable measures to ensure that the Deidentified Data cannot be associated with a natural person;
- publicly commit to maintaining and using Deidentified Data without attempting to re-identify the data;
- not make any attempt to reidentify any Deidentified Data; and
- not sell any Deidentified Data.

**4. Compliance Certification.** Upon VCI's request, Supplier will provide VCI with a certificate, signed by an officer of Supplier, certifying that:

- Supplier has completed a review of its obligations under the Privacy Program, and any corrective actions identified based upon such review or VCI's review pursuant to Section 2.2 have been completed or are underway in accordance with any corrective action plan established pursuant to Section 2.2;
- Supplier has not:
  - sold or shared Personal Information;
  - combined Personal Information received from VCI with information received from another business;
  - made any attempt to reidentify any Deidentified Data; or
  - Processed Personal Information in any way other than as necessary for the performance of the Agreement by Supplier or as expressly permitted under the Agreement.

## VW CREDIT, INC.

5. **Mobile Application Requirements.** If the performance of the Agreement by Supplier will involve the creation, management, or provision of a mobile application (“App”), Supplier will:

- validate that any App, code base, or embedded software development kit (“SDK”) is in compliance with the NIAP Protection Profile for Application Software;
- validate that any App, code base, or embedded SDK is in compliance with the OWASP Industry Standard for Mobile App Testing;
- validate that data collected by any App, code base, or embedded SDK is restricted to that communicated to end users through the privacy notice presented in-App and through the relevant application download site (e.g., App Store, Google Play, etc.), and as permitted under the Agreement;
- validate that device settings accessed by any App, code base, or embedded SDK are limited to those communicated to end users through the privacy notice presented in-App and through the relevant application download site (e.g., App Store, Google Play, etc.), and necessary to perform under the Agreement; and
- re-perform the validations set forth in this Section 5 each time any App, code base, or embedded SDK is updated and published to the general public on an application download site.

6. **Reimbursement of Costs.** Without limiting VCI’s rights or Supplier’s obligations, in the event of a breach of the Agreement with respect to Personal Information, direct damages in connection with any such breach will include the cost of any required notices; investigation, analysis, offer and provision of credit monitoring or other remediation services; call center or similar support activities; and fines or penalties.