BRdata Data Privacy Agreement

This BRdata Data Privacy Agreement ("**DPA**") amends the terms and forms, between BRdata (collectively, "**BRdata**" or "**Service Provider**"), and the **Customer** ("**Customer**" or "**you**") each a "**Party**" and collectively the "**Parties**". This DPA governs your use of BRdata products and services, including but not limited to BRdata Cloud. This DPA applies to and takes precedence over any associated contractual document between the Parties, such as Terms and Conditions, an order form, statement of work, or other thereunder (collectively, the "**Agreement**"), to the extent of any conflict. However, nothing in this DPA expands either Party's liability beyond the limits in the Agreement.

If you are an individual who consents to the terms of this DPA on behalf of an entity, you represent and warrant that you have the authority to bind that entity to this DPA and your consent to this DPA will be treated as the consent of the business.

BRdata and Customer agree as follows:

1. **Definitions**. For purposes of this DPA:

    a. "**Data Privacy Laws**" means all applicable laws, regulations, and other legal or self-regulatory requirements in any jurisdiction relating to privacy, data protection, data security, communications secrecy, breach notification, or the Processing of Personal Data, including without limitation, to the extent if and when applicable, each of the Consumer privacy acts listed on Exhibit "A" annexed hereto (each, a "CPA"). For the avoidance of doubt, if Customer's processing activities involving Personal Data are not within the scope of a given Data Privacy Law, such law is not applicable for purposes of this DPA.

    b. "**Data Controller**" or "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; for the purposes of this DPA, where Customer acts as processor for another controller, it shall in relation to the BRdata Service be deemed as additional and independent Controller with the respective controller rights and obligations under this DPA.

    c. "**Data Subject**" means an identified or identifiable natural person about whom Personal Data relates.

    d. "**Personal Data**" includes "personal data," "personal information," and "personally identifiable information," and such equivalent terms as defined by the Data Privacy Laws.

    e. "**Processing**" or "**Process**" means any operation or set of operations which is performed on Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

    f. "**Security Breach**" means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.

g. "**Service Provider**" or "**Data Processor**" has the same meaning as set forth in the applicable CPA. For the purpose of this Agreement, the Service Provider is BRdata.

2. **Scope and Purposes of Processing**.

a. BRdata will Process the Customer's data, including Personal Data, solely to fulfill its obligations to the Customer as Service Provider, on behalf of the Customer and in the course of providing the BRdata Services under the Agreement and for no other purposes, unless otherwise required by applicable Data Privacy Laws.

b. Without limiting the foregoing, Customer determines the purpose and means of Processing Customer's data. The Customer directs BRdata to Process data, including Personal Data, in accordance with the Customer's written instructions and BRdata may rely upon those directions.

- Governance. BRdata acts as a Processor and Customer and the person that it permits to use the BRdata Service ("**Authorized User**") act as Data Controllers as defined by the CPA. Customer acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of Personal Data in accordance with this DPA, including, where applicable approval by Controllers to use the BRdata Service as a Processor. Where authorizations, consent, instructions or permissions are provided by Customer these are provided not only on behalf of the Customer but also on behalf of any other Controller using the BRdata Service. Where BRdata informs or gives notice to Customer, such information or notice is deemed received by those Controllers permitted by Customer to use the BRdata Service and it is Customer's responsibility to forward such information and notices to the relevant Controllers.

- Effective Date. This DPA shall come into effect from the latest date of the acceptance by both Parties.

- Anticipated duration of Processing ("**Term**"). For the term of the Agreement or to the extent that BRdata continues to Process Personal Data, whichever is longer.

- Termination. Upon termination of this DPA, upon the Data Controller's written request, or upon fulfillment of all purposes agreed in the context of the BRdata Service whereby no further processing is required, BRdata will delete all Personal Data as described in Section 8(b) of this DPA.

3. **Customer's Role**

a. As Controller, the Customer determines the purpose and means of processing Personal Data in relation to its access and use of the BRdata Services and will provide Personal Data solely for the purpose of the Agreement. Customer agrees that: (a) it has provided all notices and obtained all consents, permissions and rights necessary under all applicable Data Privacy Laws for BRdata to lawfully process the Personal Data; (b) Customer will not transmit to BRdata nor require BRdata to process any highly sensitive data; and (c) Customers shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

b. The Customer understands that BRdata does not access or control the Personal Data made available by the Customer on the BRdata Services and in the event the Customer is not able to comply with its responsibilities under this Section 3, under any applicable Data Privacy Laws, the Customer shall notify BRdata accordingly and without undue delay.

c. Customers hereby certifies that it understands its legal and/or other restrictions and obligations set forth in this DPA and will comply with them in all respects.

4. **BRdata's Obligations**

a. BRdata will not:

- Sell Personal Data. At all times, BRdata is prohibited from "selling" as that term is defined by the applicable Data Privacy Laws, any Personal Data provided by Customer or Customer's Data Subjects.

- Process Personal Data for any purpose other than for the specific purposes set forth herein and only as necessary to perform its obligations under the Agreement. For the avoidance of doubt, BRdata will not use, retain, or disclose any Personal Data provided by Customer for any purpose other than the purposes set forth in the Agreement and this DPA including, without limitation, using the Personal Data for any business purpose other than what is set forth in this Agreement.

- Disclose Personal Information except as necessary to comply with applicable laws and regulations or to detect security incidents or prevent fraudulent activity or comply with a valid and binding order of a law enforcement agency (such as a subpoena or court order). If a law enforcement agency sends BRdata a demand for Personal Data, BRdata will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, BRdata may provide Customer's basic contact information to the law enforcement agency. If compelled to disclose Personal Data to a law enforcement agency, then BRdata will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless BRdata is legally prohibited from doing so.

- Attempt to retain, use, or disclose Customer Data for any other purpose than furthering the business purposes of this Agreement and in performance of the BRdata Services.

b. Personnel. BRdata ensures that its personnel have received appropriate training on their responsibilities concerning Personal Data as set forth in this Agreement.

5. **Compliance with Data Privacy Laws**. Each party will comply with all applicable Data Protection Laws and Regulations binding upon it in the provision or use of the BRdata Services under this Agreement, including all statutory requirements relating to data protection.

6. **Personal Data Processing Requirements**.

a. The Parties understand and agree that the BRdata Services provide Customer with security controls to enable Customer to retrieve, correct, delete, or block Personal Data and to respond to

any Data Subject Requests (as defined below). Customer is responsible for: (a)setting up and using all safety measures made available by BRdata in connection with the BRdata Services (including all security controls), and; (b) taking such steps as Customer considers adequate to maintain appropriate security, protection, deletion and backup of Personal Data, which may include use of encryption technology to protect Personal Data from unauthorized access and routine archiving of Personal Data; (c) and ensuring that users duly authorized by Customer to use the BRdata Services on behalf of Customer understand and comply with the Agreement including the DPA.

b. Cooperation. At Customer's request, BRdata will reasonably cooperate with and assist Customer and Controllers in dealing with requests from Data Subjects or regulatory authorities regarding BRdata's processing of Personal Data or any Personal Data Breach.

c. BRdata will implement and maintain policies and procedures to allow it to promptly comply with any Customer or Data Subject Requests related to a Data Subject's request to "opt-out," delete, request access to, or exercise any other rights granted to the Consumer under the CCPA and to maintain any records of such requests. Such policies and procedures will include any processes necessary to identify the specified Personal Data when responding to a particular request. If BRdata receives a request for access, a request to know, or request to delete Personal Data directly from a Data Subject, BRdata shall either act on behalf of Customer in processing the request(s) or inform the Data Subject that the request(s) cannot be acted upon because the request(s) was sent to a Service Provider.

d. BRdata shall promptly comply with any Data Subject's request to "opt-out" of the sale of that Data Subject's Personal Data, whether such request is relayed by the Data Subject or otherwise relayed by Customer.

e. Each party is responsible for its compliance with its documentation requirements, in particular maintaining records of processing where required under any applicable Data Privacy Laws. Each party shall reasonably assist the other party in its documentation requirements, including providing the information the other party needs from it in a manner reasonably requested by the other party (such as using an electronic system), in order to enable the other party to comply with any obligations relating to maintaining records of processing.

7. **Data Security**.

a. BRdata has implemented and will apply the technical and organizational measures set forth in Exhibit B. Customer has reviewed such measures and agrees that as to the BRdata Services selected by Customer under the Agreement, the measures sufficient and are appropriate taking into account the state of the art, the costs of implementation, nature, scope, context and purposes of the processing of Personal Data.

b. Changes. BRdata applies the technical and organizational measures set forth in Exhibit B to BRdata's entire customer base hosted out of the same data center and receiving the same Services. BRdata may change the measures set out in Exhibit B at any time without notice so long as it maintains a comparable or better level of security. Individual measures may be replaced by new measures that serve the same purpose without diminishing the security level protecting Personal Data.

c. Customer is solely responsible for reviewing the information made available by BRdata relating to the control of data and to data security in relation to BRdata Services and making an

independent determination as to whether the BRdata Services meet Customer's requirements, and for ensuring that Customer's personnel and consultants follow the guidelines they are provided regarding data security.

8. **Data Export And Deletion**.

a. Export and Retrieval by Customer**.** During the Term and subject to the Agreement, Customer can access the Personal Data at any time. Customer may export and retrieve its Personal Data in a standard format and subject to any Data Privacy Laws. Export and retrieval may be subject to technical limitations, in which case BRdata and Customer will find a reasonable method to allow Customer access to Personal Data.

b. Deletion**.** Before the Term expires, Customer may use BRdata' self-service export tools (as available) to perform a final export of Personal Data from the BRdata Services (which shall constitute a "return" of Personal Data). Before the Term expires, Customer is required to use BRdata's self-service export tools (as available) to perform a final export of Personal Data from the BRdata Services (which shall constitute a "return" of Personal Data) and shall delete Personal Data from the BRdata Services using the BRdata self-service tools. If Customer is unable to download and/or delete Personal Data due to any technical reason, then Customer may request that BRdata deletes or returns the Personal Data remaining on the BRdata Services.

9. **Security Breach**.

a. Notification. If BRdata becomes aware of a Security Breach, BRdata will without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify Customer of the Security Breach. Where the notification to the Customer is not made within 72 hours, it shall be accompanied by reasonable reasons for the delay.

b. Assistance. To assist Customer in relation to any data breach notifications, BRdata will include in the notification under section 10(a) such information about the Security Breach as BRdata is reasonably able to disclose to Customer, taking into account the nature of the BRdata Services, the information available to BRdata, and any restrictions on disclosing the information, such as confidentiality.

c. Limitations. Customer agrees that: (a)an attempted but failed Security Breach will not be subject to this Section; and (b) the provisions set forth in this Section 8 are not and will not be construed as an acknowledgement by BRdata of any fault or liability of BRdata with respect to the Security Breach.

10. **Subprocessors**.

a. Permitted Use. BRdata is granted a general authorization to subcontract the processing of Personal Data to Subprocessors, provided that:

- BRdata shall engage Subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the Subprocessor's processing of Personal Data. BRdata shall be liable for any breaches by the Subprocessor in accordance with the terms of this Agreement;

- BRdata will evaluate the security, privacy and confidentiality practices of a Subprocessor prior to selection to establish that it is capable of providing the level of protection of Personal Data required by this DPA; and

- BRdata' list of Subprocessors in place on the effective date of the Agreement is published by BRdata. Upon request, BRdata will make the list of Subprocessors available to Customer including the name, address and role of each Subprocessor BRdata uses to provide the BRdata Service.

b. New Subprocessors**.** BRdata's use of Subprocessors is at its discretion, provided that:

- BRdata will inform Customer in advance (by email or by posting within the BRdata Services) of any intended additions or replacements to the list of Subprocessors including name and role of the new Subprocessor; and

- Customer may object to such changes as set out in Section 11(c) herein.

c. Objections to New Subprocessors**.**

- If Customer has a legitimate reason under Data Privacy Law to object to the new Subprocessors' processing of Personal Data, Customer may terminate this Agreement (limited to the BRdata Services for which the new Subprocessor is intended to be used) on written notice to BRdata. Such termination shall take effect at the time determined by the Customer which shall be no later than thirty days from the date of BRdata's notice to Customer informing Customer of the new Subprocessor. If Customer does not terminate within this thirty day period, Customer is deemed to have accepted the new Subprocessor.

- Within the thirty day period from the date of BRdata's notice to Customer informing Customer of the new Subprocessor, Customer may request that the parties come together in good faith to discuss a resolution to the objection. Such discussions shall not extend the period for termination and do not affect BRdata's right to use the new Subprocessor(s) after the thirty day period.

- Any termination under this Section 11(c) shall be deemed to be without fault by either party and shall be subject to the terms of the Agreement.

d. Emergency Replacement**.** BRdata may replace a Subprocessor without advance notice where the reason for the change is outside of BRdata's reasonable control and prompt replacement is required to protect the integrity and security of Customer's Personal Data. In this case, BRdata will inform Customer of the replacement Subprocessor as soon as possible following its appointment.

e. Affiliates. BRdata may engage any of its affiliates to process Personal Data without seeking any prior approval from Customer. The same data protection requirements and obligations, as set forth in this DPA shall equally apply to the processing of Customer's Personal Data by any BRdata's affiliate and BRdata will, at all times, remain fully liable to Customer for affiliates compliance with such requirements and obligations.

11. **Certification and Audits**.

a. Customer Audit. Customer or its independent third party auditor reasonably acceptable to BRdata (which shall not include any third party auditors who are either a competitor of BRdata or not suitably qualified or independent) may audit BRdata' control environment and security practices relevant to Personal Data processed by BRdata only if:

- BRdata has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the BRdata Service through providing either: (i) a certification as to compliance applicable standards (scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 or other SOC1-3 attestation report. Upon Customer's request audit reports or ISO certifications are available through the third party auditor or BRdata;

- A Personal Data Breach has occurred;

- An audit is formally requested by Customer's data protection authority; or

- An applicable Data Protection Law provides Customer with a direct audit right and provided that Customer shall only audit once in any twelve month period unless mandatory Data Privacy Laws requires more frequent audits.

b. Scope of Audit. Customer shall provide at least sixty (60) days advance notice of any audit unless mandatory Data Privacy Laws or a competent data protection authority requires shorter notice. The frequency and scope of any audits shall be mutually agreed between the parties acting reasonably and in good faith. Customer audits shall be limited in time to a maximum of three business days. Beyond such restrictions, the parties will use current certifications or other audit reports to avoid or minimize repetitive audits. Customer shall provide the results of any audit to the BRdata Services.

c. Cost of Audits. Customer shall bear the costs of any audit unless such audit reveals a material breach by BRdata of this DPA, then BRdata shall bear its own expenses of an audit. If an audit determines that BRdata has breached its obligations under the DPA, BRdata will promptly remedy the breach at its own cost.

12. **Indemnification**. Each party indemnifies the other and holds them harmless against all claims, actions, third party claims, losses, damages and expenses incurred by the indemnified party and arising directly or indirectly out of or in connection with a breach of this DPA.

13. **Survival**. The provisions of this DPA survive the termination or expiration of this Agreement for so long as BRdata Process the Personal Data.

EXHIBIT “A”

Colorado Privacy Act (ColoPA)
California Privacy Rights Act of 2020 (CPRA)
Connecticut Act Concerning Personal Data Privacy and Online Monitoring (CTDPA)
Delaware Personal Data Privacy Act (DPDPA)
Florida Digital Bill of Rights (FDBR)
Indiana Consumer Data Protection Act (Indiana CPDA)
Iowa Consumer Data Protection Act (Iowa CDPA)
Kentucky Consumer Data Protection Act (KCDPA)
Maryland Online Data Protection Act (MODPA)
Minnesota Consumer Data Privacy Act (MNDPA)
Montana Consumer Data Privacy Act (MCPDA)
Nebraska Data Privacy Act (NDPA)
New Hampshire Privacy Act (NHPA)
New Jersey’s Act Concerning Online Services, Consumers, and Personal Data (NJDPA)
Oregon Consumer Data Privacy Act (OCPDA)
Rhode Island Data Transparency and Privacy Protection Act (RIDPA)
Tennessee Information Protection Act (TIPA)
Texas Data Privacy and Security Act (TDPSA)
Utah Consumer Privacy Act (UCPA)
Virginia Consumer Data Protection Act (VCDPA)

Exhibit B: Security Measures

1. TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define BRdata's current technical and organizational security measures. BRdata may change all or any portion of these measures at any time without notice so long as any such change maintains a comparable or better level of security.

1.1 Physical Access Control. Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use Personal Data are located.

- BRdata protects its assets and facilities using the appropriate means based on the BRdata Security Policy
- In general, buildings are secured through restricted access
- Depending on the security classification, buildings, individual areas, and surrounding premises may be further protected by additional measures. These include video surveillance, intruder alarm systems, or biometric access control systems, security staff.

1.2 System Access Control. Data processing systems are used with BRdata Cloud Services to protect them from being used without authorization.

- Multiple authorization levels are used when granting access to sensitive systems, including those storing and processing Personal Data. Authorizations are managed via defined processes.
- All personnel access BRdata' systems with a unique identifier.
- Access rights for any personnel who leave BRdata are immediately revoked.
- BRdata has established a password policy that prohibits the sharing of passwords, governs responses to password disclosure, and requires passwords to be changed on a regular basis and default passwords to be altered. Personalized user IDs are assigned for authentication. All passwords must fulfill defined minimum requirements and are stored in encrypted form. Each computer has a password-protected screensaver.
- The company network is protected from the public network by firewalls.
- BRdata uses up–to-date antivirus software at access points to the company network (for e-mail accounts), as well as on all file servers and all workstations.
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates. Full remote access to BRdata' corporate network and critical infrastructure is protected by strong authentication.

1.3 Data Access Control. Individuals gain access only to the Personal Data that they have a right to access, and Personal Data must not be read, copied, modified or removed without authorization in the course of processing, use and storage.

- All production servers are operated in in secure server rooms. Security measures that protect applications processing Personal Data are regularly checked. To this end, BRdata conducts internal and external security checks and penetration tests on its IT systems.
- An BRdata security standard governs how data and data carriers are deleted or destroyed once they are no longer required.

1.4 Data Transmission Control. Except as necessary for the provision of the BRdata Services in accordance with this Agreement, Personal Data must not be read, copied, modified or removed without authorization during transfer. Where data carriers are physically transported, adequate measures are implemented at BRdata to provide the agreed-upon service levels (for example, encryption and lead-lined containers).

- Personal Data in transfer over BRdata internal networks is protected according to BRdata Security Policy.
- When data is transferred between BRdata and its Customers, the protection measures for the transferred Personal Data are mutually agreed upon and made part of the relevant agreement. This applies to both physical and network based data transfer. In any case, the Customer assumes responsibility for any data transfer once it is outside of BRdata-controlled systems.

1.5 Data Input Control.

- BRdata only allows authorized personnel to access Personal Data as required in the course of their duty.
- BRdata has implemented a logging system for input, modification and deletion, or blocking of Personal Data by BRdata or its Subprocessors within the Cloud Services to the extent technically possible.
- BRdata can retrospectively examine and establish whether and by whom Personal Data have been entered, modified or removed from BRdata processing systems.

1.6 Job Control. Personal Data being processed on a Customer's behalf is processed solely in accordance with this Agreement and related instructions of the Customer.

- BRdata uses controls and processes to monitor compliance with contracts between BRdata and its Customers, subprocessors or other service providers.
- As part of the BRdata Security Policy, Personal Data requires at least the same protection level as "confidential" information according to the BRdata Information Classification standard.

- All BRdata employees and contractual Subprocessors or other service providers are contractually bound to respect the confidentiality of all sensitive information including trade secrets of BRdata customers and partners.

1.7 **Availability Control.** Personal Data will be protected against accidental or unauthorized destruction or loss.

- BRdata employs regular backup processes to provide restoration of business-critical systems as and when necessary.
- BRdata has defined business contingency plans for business-critical processes and may offer disaster recovery strategies for business critical Services as further set out in the Documentation or incorporated into the Statement of Work Form for the relevant Service.
- Emergency processes and systems are regularly tested.

1.8 **Data Separation Control.**

- BRdata uses the technical capabilities of the deployed software (for example: multi- tenancy, system landscapes) to achieve data separation among Personal Data originating from multiple Customers.
- Each Customer has access only to its own data.

1.9 **Data Integrity Control.** Personal Data will remain intact, complete and current during processing activities.

BRdata has implemented a multi-layered defense strategy as a protection against unauthorized modifications. These measures are designed to reduce risk and do not guarantee the elimination of all security incidents.

In particular, BRdata uses the following to implement the control and measure sections described above:

- Firewalls;
- Security Monitoring Center;
- Antivirus software;
- Backup and recovery;
- External and internal penetration testing;
- Regular external audits to prove security measures.