

Data Processing Agreement (Particle IoT)

Parties and Scope

This Data Processing Agreement (“**DPA**”) is entered between **Particle Industries, Inc.** (doing business as Particle IoT, hereinafter “**Particle**”), and the **Customer** (the entity that has engaged Particle’s services). The Customer is the “Data Controller” and Particle is the “Data Processor” as defined under applicable data protection laws (e.g., the EU General Data Protection Regulation, **GDPR**). This DPA applies to Particle’s processing of Personal Data on behalf of the Customer in providing the Particle IoT platform and related services (“**Services**”). It forms part of the overall agreement between Customer and Particle for use of the Services. All capitalized terms not defined here shall have the meanings given in the applicable privacy laws or the main service agreement.

Subject Matter and Duration

Subject Matter: Particle will process certain personal data strictly for the purpose of providing and supporting the IoT connectivity, device management, and related cloud services that Customer uses. This includes activities such as storing account information, facilitating device communications, providing geolocation services, and other actions **solely** to fulfill Customer’s usage of Particle’s platform. Particle **will not** process the personal data for any independent purposes other than those instructed by Customer or as required by law.

Duration: The processing shall continue for the duration of the Customer’s use of Particle’s Services and until all personal data is deleted or returned to the Customer as described in this DPA. In practice, Particle will retain personal data for as long as the Customer’s account remains active and the Services are provided. If the Customer’s account is terminated or becomes inactive, Particle will delete or return the personal data upon termination (with allowances for any retention required by law or for legitimate business purposes, such as resolving billing issues), as further detailed in the **Deletion** section below.

Nature and Purpose of Processing

Particle shall process personal data **only** for the purposes of delivering the Services to the Customer. The nature of processing includes collection, storage, and use of personal data needed to:

- Create and manage Customer’s accounts and authenticate users;
- Enable Customer’s IoT devices to connect to Particle’s cloud platform (including network connectivity via SIM cards, device messaging, event logging, etc.);

- Provide real-time data communications and location services (e.g. processing device GPS coordinates for location tracking features);
- Allow web or app access (such as processing user agent and IP information for security, interface customization, or troubleshooting); and
- Provide customer support, billing, and administrative services related to the Customer's account.

Particle will process the data **only on documented instructions** from the Customer (as set out in this DPA, the service agreement, and through Customer's use of settings in the platform), and **not for Particle's own purposes**. Particle **will not "sell" or share personal data** to third parties for marketing or other independent use, and will not derive analytics or profiling on data subjects for Particle's benefit, except as needed to provide the Services as instructed. The processing is **necessary** for Particle to perform its obligations and provide the functionality requested by the Customer.

Types of Personal Data

The personal data that Particle processes on behalf of Customer is limited to the categories relevant for IoT account management and device operations. This may include:

- **Contact Information:** e.g. full name, email address, and mailing or billing address of Customer's account owners or users .
- **Account and Identifiers:** e.g. usernames and account IDs for the Particle platform, as well as device identifiers and SIM card IDs associated with Customer's IoT devices .
- **Technical Usage Data:** e.g. IP addresses from which devices or users connect to the Service, and browser or app information such as user agent strings .
- **Geolocation Data:** e.g. GPS coordinates or approximate location data transmitted by Customer's devices (if the Customer uses Particle's location services) .

Particle **does not** intentionally collect or store any other personal data of end-users or consumers of the Customer. In particular, Particle does not gather sensitive personal information or any personally identifiable information about the Customer's own customers or end-users beyond the technical device data listed above. The Customer should refrain from using the Services to send or store any personal data that is not covered by the categories above without notifying Particle and ensuring compliance with applicable law. If Customer's use of the Services requires processing additional personal data types or data subject categories not described here, the Customer must inform Particle and obtain necessary approvals or an amendment to this DPA.

Categories of Data Subjects

The data subjects whose personal data is processed under this DPA include:

- **Customer's Team Members:** Individuals who act as Customer's users of the Particle platform, such as the Customer's employees, contractors, or other personnel authorized to access the account and manage devices. These individuals provide their personal information (name, contact info, etc.) to create accounts and use the Services.
- **Device Owners/Operators:** In cases where IoT devices are personal or associated with individuals, the individuals who operate or carry those devices may indirectly be data subjects (for example, if a device transmits its geolocation which relates to a person's location). However, Particle typically processes such data as technical device information without identifying the individual. Particle does not maintain a direct relationship with the Customer's end-users; any personal data about end-users contained in device data is incidental and controlled by the Customer.

Aside from the above, Particle's Services are **not intended to be used to process data about the Customer's customers or end-consumers**. The Customer, as controller, is responsible for ensuring that any personal data of third parties (if any) included in the device data is collected and transferred to Particle in compliance with applicable laws (and with proper notice or consent obtained by the Customer). Particle will treat all personal data received from Customer as **Customer's Confidential Information** and in accordance with the terms of this DPA.

Obligations of the Customer (Controller)

The Customer, as Data Controller, agrees and warrants that:

- **Lawful Basis:** The Customer has obtained all necessary consents or has another valid legal basis for the processing of the personal data by Particle, and that the personal data has been collected and is being shared with Particle in compliance with applicable data protection laws.
- **Instructions:** The Customer will only instruct Particle to process personal data in a manner consistent with applicable laws. Any additional instructions outside the scope of the Services or this DPA must be agreed upon in writing. The Customer is responsible for ensuring that Particle is informed of any processing activities or data types that may require additional safeguards.
- **Data Accuracy:** The Customer shall provide personal data that is accurate and relevant for the specified purposes, and shall keep such data updated as necessary. If Particle becomes aware that data is inaccurate or outdated, it may inform the Customer to rectify or update it.
- **Data Subject Requests:** When appropriate, the Customer will handle any requests or complaints from its end-users or data subjects relating to their personal data (e.g. requests to access, correct, or delete data). Where Particle receives a request directly from an individual for data that Particle processes as a processor for Customer, Particle will forward it to Customer (as outlined in **Data Subject Rights** below).
- **Assessment and Compliance:** The Customer will undertake any required data protection impact assessments (DPIA) or consultations with authorities, if needed for the

Customer's use of Particle's Services. Particle will reasonably assist with providing information for such DPIAs upon request (see **Assistance** below).

- **Use Restrictions:** The Customer shall not use the Services to process any personal data that is classified as highly sensitive (e.g. health data, financial account info, government ID numbers, special categories of data under GDPR) unless there is prior written agreement with Particle. The Customer is responsible for ensuring that its use of the Services (and the personal data it instructs Particle to process) complies with all applicable privacy and data protection laws relevant to Customer's jurisdiction and data subjects.

Obligations of Particle (Processor)

As the Data Processor, **Particle** agrees to the following obligations, in accordance with Article 28 of the GDPR and other applicable laws:

- **Processing on Instructions:** Particle will process personal data **only on documented instructions** from the Customer. This DPA, along with the Service agreement and the functionality the Customer uses in the platform, constitute the Customer's complete instructions to Particle. Particle will not retain, use, or disclose the personal data for any purpose other than as instructed to perform the Services. If Particle is required by law to process data beyond Customer's instructions, Particle will inform the Customer of that legal requirement before processing (unless the law prohibits such notice).
- **Confidentiality:** Particle will ensure that any personnel or subprocessors authorized to process the personal data are under appropriate obligations of confidentiality. This means that employees handling Customer data are bound by confidentiality agreements or statutory obligations. Particle will not disclose Customer's personal data to any third party unless permitted by the Customer or this DPA, or required by law (in which case, it will notify Customer if legally allowed).
- **Security Measures:** Particle shall implement and maintain appropriate **technical and organizational security measures** to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction, damage, or breach. These measures are described in more detail in the **Data Security** section below. In summary, Particle uses industry standard practices such as data encryption, access controls, network security monitoring, and regular security assessments to safeguard personal data.
- **Sub-Processors:** Particle may engage authorized **sub-processors** (third-party service providers) to assist in processing personal data (for example, cloud hosting providers or telecommunication carriers for IoT connectivity). However, Particle will only do so under a written contract with the sub-processor that imposes the **same level of data protection obligations** as in this DPA. Particle remains fully liable to the Customer for the performance of its sub-processors. A list of current sub-processors is maintained by Particle and will be made available to Customer (e.g., via Particle's website or upon request). Particle will notify the Customer of any intended additions or replacements of

sub-processors and give the Customer the opportunity to object for legitimate grounds. (See **Sub-Processors** section below for more details.)

- **Assistance with Data Subject Rights:** Particle will promptly notify the Customer if it receives any request from an individual (data subject) regarding their personal data that Particle processes (e.g., requests to access, rectify, or erase data). Particle will **not respond directly** to such requests (unless legally compelled or if the request is clearly meant for Particle acting as a controller of other data) and will instead **assist the Customer** in responding. Upon Customer's request, Particle will provide reasonable support and information to enable the Customer to fulfill obligations to honor data subject rights under applicable laws (for example, by extracting or deleting specific user's data from the platform, or by providing log files relevant to a data subject's request).
- **Assistance with Compliance:** Taking into account the nature of processing and the information available, Particle will assist the Customer in ensuring compliance with the Customer's obligations under relevant data protection laws. This includes providing assistance with:
 - **Security and DPIAs:** Providing information about Particle's security measures and processing activities to support Customer's data protection impact assessments or consultations with regulators, if required. Particle will also assist in implementing any additional security controls reasonably required by Customer to address specific risks.
 - **Breach Response:** Notifying Customer of personal data breaches and providing cooperation and information for Customer's breach notifications (addressed in **Data Breach Notification** section).
 - **Regulatory Compliance:** Providing information required to demonstrate compliance with this DPA and allowing for audits (as detailed in **Audits and Documentation** section).
- **Return or Deletion of Data:** Upon termination or expiration of the Customer's services, or upon Customer's written request, Particle will **promptly delete or return all personal data** processed on behalf of Customer, and will delete existing copies of the data (unless storage is required by law). If return of data is requested, Particle will provide the data in a common machine-readable format. If deletion is requested (or required by the DPA), Particle will securely erase the data from its systems. In either case, Particle may retain minimal personal data to the extent required to comply with legal obligations or for backup purposes, but in all cases maintaining the data protections of this DPA until the data is deleted.
- **No Further Disclosure:** Particle shall not disclose personal data to any government, law enforcement, or other third party except as directed by Customer or strictly required by law. If a law enforcement or other governmental request for Customer's data is received, Particle will (to the extent allowed) redirect the requesting party to seek the data directly from Customer or will promptly notify Customer to allow it to seek a protective order or other appropriate remedy.
- **Liability and Indemnity:** Particle's liability arising from data processing under this DPA shall be subject to the limitations and exclusions of liability set forth in the main service agreement between Particle and Customer. Each party remains responsible for any fines

or penalties imposed due to its own non-compliance with applicable data protection laws. Both parties agree to indemnify each other to the extent the main agreement provides, for losses arising from a breach of this DPA caused by the indemnifying party's actions.

Data Security Measures

Particle recognizes the importance of protecting personal data. **Security measures** implemented by Particle include, but are not limited to:

- **Encryption:** Personal data is encrypted in transit using TLS/SSL and, where applicable, encrypted at rest on storage media. For example, web interactions with Particle's platform are over HTTPS, and sensitive database fields or backups are encrypted to prevent unauthorized access.
- **Access Controls:** Access to systems and personal data is restricted to authorized personnel on a need-to-know basis. Particle employs strong authentication (such as password policies and multi-factor authentication) for its employees and administrators. Role-based access controls ensure that each user (including Customer's users) can only access data relevant to their role.
- **Network and System Security:** Particle maintains firewalls and network segmentation to isolate databases and sensitive systems. Regular vulnerability assessments, penetration testing, and security monitoring are conducted to detect and prevent intrusions or anomalies. The infrastructure hosting Customer data (e.g., cloud servers) is hardened and kept up-to-date with security patches.
- **Monitoring and Logging:** Systems are monitored for security events, and logs of access to personal data are maintained. Particle can provide logging or audit records to Customer as needed to demonstrate data access history as part of compliance or security review.
- **Organizational Measures:** Particle's staff are trained in data protection and security practices. Internal policies are in place to handle security incidents, data confidentiality, and privacy compliance. Particle also has an appointed Privacy Officer and/or security team responsible for overseeing these measures.
- **Data Minimization and Pseudonymization:** Particle limits the personal data collected to only what is necessary for the purposes of the Services (as described above) . Where feasible, Particle may pseudonymize or aggregate data to reduce the use of identifiable personal data. For instance, Particle might reference device data by an ID number rather than a user's name in internal systems, except where needed for account management.

These measures are designed to ensure a level of security appropriate to the risk of the personal data being processed. The Customer acknowledges that it has reviewed Particle's technical and organizational measures and deems them sufficient for the protection of personal data in light of the nature of the Services. Particle will update or enhance these measures as needed to comply with evolving security standards and legal requirements, and can provide more detailed documentation of its security measures upon Customer's request.

Sub-Processors

Sub-processors are the third-party service providers that Particle engages to assist in providing the Services and that may process personal data. Particle currently uses sub-processors for functions such as cloud infrastructure hosting, data storage, and network connectivity (for example, data center or cloud service providers, telecom carriers for SIM connectivity, email service for user communications, etc.). Key sub-processors may include well-known cloud platform providers or other vendors necessary to run the Particle IoT cloud.

Particle maintains a **list of authorized sub-processors** available on our Privacy Page: <https://www.particle.io/legal/privacy/>

The Customer provides general authorization for Particle to use these sub-processors as listed and updated. In the event Particle intends to engage a new sub-processor or replace an existing one, Particle will give the Customer advance notice (for example, via email or an update to the sub-processor list) at least 30 days before the change. If the Customer has a reasonable, lawful basis to object to the new sub-processor (e.g., if adding that processor would materially weaken data protections), the Customer must notify Particle in writing within the notice period. The parties will then discuss the concerns in good faith, and if the Customer continues to object and no agreeable solution is found, the Customer may have the right to terminate the affected Services without penalty.

Particle ensures that all sub-processors are bound by **written agreements** that require them to provide at least the same level of data protection and security as Particle commits to under this DPA . Particle conducts due diligence on its sub-processors and is responsible for their compliance with the obligations under this DPA. If a sub-processor fails to fulfill its data protection obligations, Particle remains liable to the Customer for the performance of that sub-processor's obligations.

International Data Transfers

Customer acknowledges that Particle is a U.S.-based provider and that personal data will be **stored and processed in the United States** (and possibly other jurisdictions where Particle or its sub-processors maintain facilities, which currently primarily includes the USA). All personal data is hosted on servers in the USA . Authorized personnel of Particle (including those in its worldwide offices or subsidiaries) or its sub-processors may access the data remotely from outside the USA (for example, to provide support or infrastructure management), but any such access will be performed in compliance with this DPA and applicable law.

For Customers subject to EU/EEA, UK, Swiss or other international data transfer regulations, the parties shall ensure that **adequate transfer mechanisms** are in place for the lawful transfer of personal data to Particle in the USA. Such mechanisms may include:

- **Standard Contractual Clauses (SCCs):** The European Commission's approved Standard Contractual Clauses (2021 SCCs) are hereby incorporated into this DPA by reference for any transfers of Personal Data from the EEA, UK, or Switzerland to the U.S. where EU/UK data protection law applies . Specifically, if Customer is subject to GDPR and is transferring data as a controller to Particle as a processor, the parties agree to the Controller-to-Processor SCCs (Module Two) by default . If Customer is a processor for another controller and Particle is a sub-processor, the Processor-to-Processor SCCs (Module Three) apply. These clauses will be deemed executed by the parties upon acceptance of this DPA. In case of conflict between the SCCs and any other part of this DPA, the SCCs will prevail to the extent of the conflict .
- **EU-U.S. Data Privacy Framework (DPF):** Particle has certified compliance with the EU-U.S. and Swiss-U.S. Data Privacy Framework as administered by the U.S. Department of Commerce (if applicable) . This means Particle commits to uphold the DPF Principles for relevant personal data transferred from the EU/Switzerland to the U.S., including cooperation with European data protection authorities. Where the DPF is recognized as a valid transfer mechanism, Customer agrees that Particle's DPF certification can be relied upon for data transfers.
- **Additional Safeguards:** Particle commits to implementing supplementary measures as needed to protect data transferred to the U.S., such as encryption in transit and at rest, strict access controls, and policies for handling government data requests. Particle will also, upon request, provide information about any government access to personal data and any risk assessments performed (consistent with what is allowed under law).

By using Particle's Services, the Customer authorizes Particle to transfer and process personal data globally as needed to provide the Services, subject to the foregoing safeguards. Customer is responsible for notifying data subjects of these international transfers as required by law. Particle will cooperate with Customer to address any regulatory inquiries or challenges regarding international transfer of personal data (for example, responding to requests from European data protection authorities about how data is protected in the U.S.).

Data Subject Rights and Requests

Particle is committed to assisting the Customer in fulfilling obligations to data subjects who wish to exercise their privacy rights. If Particle receives any communication directly from an individual (such as an end-user or a Customer employee) regarding the processing of their personal data – for example, a request for access to data, correction of data, deletion (right to be forgotten), restriction of processing, data portability, or an objection to processing – Particle will **promptly inform the Customer**. Because Particle acts as a processor, it will **not respond to the request directly** (unless legally required, or if the request pertains to data Particle controls outside of this DPA), and will instead defer to Customer's instructions on how to proceed.

Upon Customer's request, Particle will **assist** the Customer by providing available information or tools needed to fulfill the data subject's request. For instance:

- If a data subject requests a copy of their personal data, Particle can export the relevant personal data from the platform in a structured, commonly used format and provide it to Customer to furnish to the data subject.
- If a data subject requests deletion or correction, Particle will, upon Customer's instruction, delete or correct the personal data within Particle's systems (to the extent technically feasible) and confirm the action.
- If a data subject objects to processing or withdraws consent (where consent was the basis), Particle will support Customer in implementing any required restriction on processing (for example, disabling the user's account or stopping certain data collection on Customer's devices if technically possible).

Particle has established procedures to ensure that such requests can be addressed promptly. The Customer is responsible for communicating the outcome of the request to the data subject and handling any related communications. Particle will not charge additional fees for reasonable assistance with data subject requests, provided the volume of requests is not excessive. In the event of unusually burdensome or frequent requests, the parties will discuss in good faith an appropriate solution (which may include a reasonable fee if permitted by law).

Both parties shall maintain records of data subject requests and how they addressed them, as required by law. Particle will notify Customer immediately if it believes an instruction related to a data subject request violates any applicable data protection law, so that the parties can resolve the issue in accordance with the law.

Data Breach Notification

In the event that Particle becomes aware of a **personal data breach** affecting Customer's personal data, Particle will notify the Customer **without undue delay** (and in any case promptly, taking into account the need to verify initial facts, but aiming to do so within 48 hours). A "personal data breach" means any confirmed incident leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed by Particle.

The notification to Customer will include (to the extent known at the time):

- A description of the nature of the breach, including the categories and approximate volume of personal data and individuals concerned.
- The likely consequences and risks for data subjects as a result of the breach.
- The measures already taken or proposed by Particle to address the breach, including actions to mitigate its possible adverse effects.
- Contact information for a Particle incident response coordinator who can provide further information.

Particle will promptly take all reasonable steps to contain, investigate, and remediate the data breach. It will cooperate with Customer's reasonable requests in relation to the breach, including

providing information for Customer to fulfill any **legal reporting obligations**. For example, under GDPR the Customer (as controller) must notify supervisory authorities and/or data subjects of certain breaches within specific timeframes; Particle will assist Customer by providing the necessary details about the breach and actions taken .

The parties agree to coordinate in good faith on breach response. Particle will not make any public statements (e.g., press releases) or notifications to affected individuals or regulators about the breach that reference the Customer, without the Customer's prior consent, unless required by law. Conversely, if Customer is required to make such notifications, Particle will provide input on the content as relevant to the portion of the incident related to Particle's Services.

Notification of a breach by Particle to Customer shall not be construed as an acknowledgment by Particle of any fault or liability for the incident. Both Particle and Customer shall document the facts relating to any data breaches, their effects, and the remedial actions taken, and will maintain such records as required by law.

Data Retention and Deletion

Particle will not retain personal data **longer than necessary** for the purposes of processing. By default, Particle retains the Customer's personal data for the duration of the service relationship. Active account data remains stored for as long as the Customer's account is active in order to provide the Services (which, as noted, can span many years, potentially 10+ years or more for long-term IoT deployments).

Upon termination of the Services or at an earlier time upon Customer's instruction, Particle will take the following steps regarding personal data:

- **Return of Data (Optional):** At Customer's request, Particle can export and return all personal data to the Customer. This may include account information and any device or usage data that is considered personal data. The data will be provided in a reasonable format (such as CSV, JSON, or a database export), ensuring that Customer can restore or migrate the data to their own systems.
- **Deletion:** After data return (if requested) or directly upon termination if no return is requested, Particle will proceed to **securely delete** the personal data from its systems. Deletion involves removing data from databases, overwriting or wiping storage media, and deleting backups, in accordance with Particle's data destruction policies. Particle will confirm to Customer in writing that deletion has been completed upon Customer's request.

Exceptions: Particle may retain personal data (in a secure manner) if required to do so by applicable law or legitimate business needs. For example, Particle might retain minimal information for tax or billing records, or to comply with a legal obligation or court order. Any

retained data will continue to be protected under the terms of this DPA and applicable laws, and will only be retained for the period necessary under such obligation.

Additionally, certain data that is stored in backups or archival systems may not be immediately deleted (due to technical infeasibility), but Particle will ensure such data is isolated and securely protected until it is overwritten or erased in the ordinary course of backup rotation. Particle will not use any retained data for any other purpose than compliance with law or defense of legal claims.

The Customer is responsible for downloading or requesting return of any data it wishes to retain **before** the end of the service term or termination of the account. Particle will, to the extent practicable, provide a reminder or assistance to facilitate data export prior to deletion. Once deleted, data may not be recoverable.

Audits and Documentation

Particle will provide Customer with **reasonable evidence** of compliance with the obligations set out in this DPA. This may include providing copies of relevant third-party certifications, audit reports, or summaries of test results that Particle undergoes. For example, Particle maintains certifications or compliance attestations (such as SOC 2) and can furnish copies or reports to Customer upon request to demonstrate that appropriate controls are in place.

Additionally, Particle will respond to legitimate Customer inquiries regarding its data processing and protection practices. Particle has documentation (policies, procedures, records of processing activities) that can be made available to the Customer as needed to reasonably verify Particle's compliance.

If the Customer is required by law or regulation to verify Particle's processing (for instance under GDPR Article 28, the controller has the right to audit the processor), the Customer may **conduct an audit or inspection**. Such audits:

- Must be pre-scheduled with at least 30 days advance written notice to Particle (generally, 2-4 weeks' notice is typical to arrange logistics and security).
- Will be conducted no more than once per year, except in case of specific concerns or evidence of non-compliance, or if required by a supervisory authority.
- Can be performed either by the Customer itself or by an independent auditor chosen by Customer and acceptable to Particle (requiring the auditor to be bound by confidentiality).
- Should be limited in scope to matters relevant to this DPA and performed in a manner that does not disrupt Particle's business operations or compromise other customers' data. For example, the audit may involve review of Particle's security controls, policies, and perhaps on-site visits or interviews with relevant personnel, but cannot permit access to data of other customers.

Particle will cooperate with the audit and provide access to the necessary information, personnel, and facilities. The Customer will be responsible for its costs of the audit, and Particle will allow the audit at no charge except if the audit requests are excessive or beyond standard practice (in which case the parties will negotiate a reasonable fee for support).

If an audit identifies any material deficiencies in Particle's compliance with this DPA, Particle will take prompt corrective action at its own expense. The parties will mutually agree on a remediation plan to address any findings. Particle will also report back when the remediation is completed.

All information obtained or observed by Customer or its auditors during an audit must be kept confidential and used solely for the purpose of assessing compliance. This includes any reports or results from the audit. Upon request, the parties may agree to share the summary of audit results with Customer's relevant regulators if needed to demonstrate compliance.

Miscellaneous Provisions

- **Conflict with Other Agreements:** In the event of any conflict between this DPA and any other agreement between the parties (including the main service Terms of Use or Privacy Policy), the provisions that provide greater data protection to individuals or impose stricter obligations on Particle will prevail with regard to the subject matter of processing personal data. Otherwise, this DPA is subject to the liability limitations and other general terms of the main agreement between Particle and Customer.
- **Governing Law:** This DPA shall be governed by and interpreted in accordance with the same law and jurisdiction as stipulated in the main service agreement between the parties, unless required otherwise by applicable data protection laws.
- **Changes and Updates:** Particle may update this DPA from time to time, for example, to comply with changes in law or to include additional safeguards. No material reduction in data protection rights will be made in any update. In case of significant changes, Particle will notify the Customer and, if required, seek Customer's agreement. The current version of the DPA will be made available to Customer through Particle's website or support channels.
- **Severability:** If any provision of this DPA is found to be invalid or unenforceable, the remainder of this DPA shall remain in full effect. The parties will replace any invalid provision with a valid one that most closely approximates the intent and economic effect of the invalid provision.
- **Entire Agreement:** This DPA (including any attachments like Standard Contractual Clauses, if applicable) constitutes the entire agreement between Customer and Particle with regard to the processing of personal data in the context of the Services, and supersedes any prior agreements or understandings on the same subject. In no event shall any party's standard business terms (e.g., purchase order terms) modify the terms of this DPA.

By using Particle's Services or by otherwise signing or accepting this DPA, the Customer and Particle each acknowledge and agree to the terms above. Each party's authorized representative has the full legal authority to bind the party to this DPA. This DPA is effective as of the date of the Customer's acceptance (either by signature or by electronic acceptance as part of the service agreement).