Data Processing Agreement

Version: September 27th, 2023

1. General

1.1 Words like **IXON**, **we, us,** or **our** in this Data Processing Agreement, shall refer to:

- **IXON B.V.**, a Dutch corporation, if your company is located outside of the United States of America and Canada; IXON B.V. has a principal place of business at the Zuster Bloemstraat 20, 5835 DW, in Beugen, the Netherlands, and is registered with the Dutch Chamber of Commerce under file number 62729918.; or
- **IXON Inc.**, a Delaware corporation, if your company is located within the United States of America or Canada, IXON Inc.; IXON Inc. has a mailing address at 228 E. 45 Street, Suite 9E, New York, NY 100017, USA.

1.2 If your company is located outside of the United States of America and Canada, this agreement is between you and IXON B.V. If your company is located within the United States of America or Canada, this agreement is between you and IXON Inc.

1.3 We offer cloud-based services on our IXON Cloud for remote access to, as well as monitoring of, machines and systems connected to the internet via an edge gateway. These services may also be provided on a white label basis. In any case accounts are needed to be able to login to and use our cloud-based services. For this purpose, certain personal data of our customer's employees, the personnel of our customer's clients, and/or third parties given access by you or your clients is processed by us.

1.4 Words like **you**, **your** and **customer** in this Data Processing Agreement shall refer to you or our customer who has executed an agreement with us for the provision of certain services. You acknowledge and agree that the resulting processing of personal data is subject to the General Data Data Protection Regulation (Regulation (EU) 2016/679, hereinafter: '**GDPR**'). This Data Processing Agreement applies insofar you can be qualified as a 'Data Controller' under the GDPR, and we can be qualified as a 'Data Processor' under the GDPR.

1.5 We are entitled to change this Data Processing Agreement with your consent. Consent to such a change shall be deemed to have been given if we notify you of the amendment in writing (which includes email) and you do not object to the amendment within four weeks of receiving the amendment notification. Parties agree not to amend this Data Processing Agreement in a way that detracts from the fundamental rights or freedoms of data subjects.

1.6 Unless we expressly agree to their validity in writing, your deviating, conflicting or supplementary terms or conditions shall not become part of any agreement between you and IXON, even if we do not expressly object to their inclusion.

1.7 Where, in this Data Processing Agreement, reference is made to terms that are defined in the GDPR, such as 'data controller', 'data processor' and 'personal data', such terms shall have the meanings given to them in the GDPR.

1.8 In the event of a contradiction between these terms and the provisions of related agreements between the Parties, existing at the time these terms are agreed or entered into thereafter, this Appendix, meaning only the terms of 'Appendix I: Data Processing Agreement' and expressly not of the Terms of Use, shall prevail.

1.9 Appendix II: Technical and Organizational Measures and Appendix III: List of sub-processors form an integral part of this Data Processing Agreement.

2. Description of processing

2.1 IXON undertakes to process personal data on behalf of you, the data controller, in accordance with the conditions laid down in this Data Processing Agreement, unless required to do so by Union or

Member State law to which we are subject. The processing will be executed: (i) within the framework of the agreements between you and us, including our Terms of Use, and (ii) for all such purposes reasonably related thereto and as may be agreed to subsequently.

2.2 The personal data processed by us, and the categories of data subjects to whom the personal data relates, are specified below:

- Categories of data subjects:
  - Your (external) personnel who you instruct and allow to use our services.
  - Personnel and/or external personnel of your clients who you provide (white labeled, if applicable) services to.
  - Third parties who are given access to our services by your or your clients.
- Categories of personal data:
  - Device information (IP address, MAC address, browser data), name, email address, the date and time of visit and location.
- Duration of processing:
  - As long as needed to perform our obligations under any agreement between you and IXON.
  - At your choice, we will delete or return all the personal data to you after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the personal data.

2.3 We shall refrain from making use of the personal data for any other purpose than as agreed upon with you. You shall inform us of any processing purposes which are not clearly mentioned in this Data Processing Agreement or which are not a logical consequence of the agreed upon services. However, under our own responsibility, we are entitled to process personal data for analytical purposes and service improvement.

2.4 We shall not take any unilateral decisions about the processing of personal data for other purposes. The control over the personal data processed under this Data Processing Agreement rests with you as the data controller. All personal data processed on your behalf shall remain your property or the property of the relevant data subjects.

3. Obligations & Responsibilities

3.1 Regarding the processing of personal data mentioned in the previous article, we shall use all commercially reasonable efforts to ensure compliance with applicable laws and regulations governing the protection of personal data, such as the GDPR.

3.2 A list of technical and organizational measures we use to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons, can be found in Appendix II: Technical and Organizational Measures.

3.3 Our obligations arising from this Data Processing Agreement also apply to those processing personal data under our authority, including but not limited to our employees.

3.4 We will provide any reasonably necessary assistance if a data protection impact assessment, or a prior consultation with a supervisory authority, is necessary with respect to the processing of personal data.

3.5 As the processor of personal data, we are responsible for the processing that takes place within the scope of this Data Processing Agreement and your reasonable instructions. We are not responsible for other processing of personal data, including but not limited to, your collection of personal data and processing for purposes that are not mentioned in this Data Processing Agreement.

3.6 You represent and warrant that you have a valid legal basis to process, and have us process, the personal data. Furthermore, you represent and warrant that the content, the use and the instruction to process the personal data within the meaning of this Data Processing Agreement are not unlawful and do not infringe any rights of a third party. In this context, you indemnify us and hold us harmless

from and against claims and actions of such third parties relating to the processing of personal data.

3.7 On request, you shall make a copy of these terms available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information you may redact part of the text of these terms prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

4. Transfer of personal data

4.1 You hereby grant us permission to process the personal data in countries within the European Economic Area. In addition, we may transfer the personal data to a country outside the European Economic Area provided that such country guarantees an adequate level of protection and/or all other obligations under this Data Processing Agreement and the GDPR are complied with.

4.2 At your request, we shall inform you about the countries in which the personal data is processed. You are always entitled to object to any processing of personal data outside of the European Economic Area. We shall take such objections seriously and will try to find a reasonable solution. If we cannot come to a solution that is acceptable for both parties, and the continued transfer of personal data is in breach of any privacy legislation applicable to you as a controller, then you are entitled to terminate your agreements with us.

5. Third parties and subcontractors

5.1 You hereby grant us general permission to engage third parties (sub-processors) within the scope of the services we provide to you. At your request, we shall inform you about the engaged sub-processors and/or any plans to engage new sub-processors. A list of used sub-processors can be found in Appendix III.

5.2 In any case, we shall proactively inform you of any intended changes concerning the engagement of new sub-processors. When we have informed you about such a change in sub-processors, you shall have one month to object in writing to our communicated intentions. If you object to our intention to engage a new sub-processor, then the parties agree to engage in good faith discussions to resolve the matter. If the parties do not reach an agreement on our intention to engage the sub-processor, then we may engage the relevant new sub-processor and you will be entitled to terminate your agreement with us by the date on which the new sub-processor is engaged. If you do not object to our communicated intentions within the four-week term, then you shall be deemed to have no objections to the change in sub-processors.

5.3 When engaging sub-processors, we shall ensure that such sub-processors will be obliged to agree in writing to duties which are substantially the same as agreed in this Data Processing Agreement.

5.4 We shall remain fully responsible to you for the performance of the sub-processor's obligations under its contract with us. We shall notify you of any failure by the sub-processor to fulfill its obligations under that contract.

6. Security

6.1 Parties shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and

the risks involved in the processing for the data subjects. We shall implement the technical and organizational measures specified in Appendix II to ensure the security of the personal data.

6.2 We shall grant access to the personal data to members of our personnel only to the extent strictly necessary for the implementation, managing and monitoring of our services. We shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6.3 We shall periodically review and update our technical and organizational security measures to make sure that these measures remain at an appropriate level considering changes (if any) in the state of technology and the nature of the personal data. We do not warrant that the security measures are effective under all circumstances. At your request, we shall provide you with our latest information regarding our implemented security measures.

7. Data breaches

7.1 In the event of a personal data breach concerning personal data processed by us under these terms, we shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects. We will notify you of the breach without undue delay but at least within forty-eight (48) hours upon its discovery. You, as the controller of the personal data, shall solely decide whether or not to notify the data subjects and/or the relevant supervisory authorities about the data breach.

7.2 If required by applicable laws and/or regulations, we shall provide all reasonable cooperation in notifying the relevant authorities and/or data subjects. However, you remain the responsible party for any statutory notification obligations in respect thereof.

7.3 In case of a data breach, we shall provide you with the information necessary for you to comply with your legal notification obligations towards data subjects and/or authorities. The notification obligation includes in any event the duty to report the fact that a breach has occurred, including details regarding:

- the (suspected) cause of the breach;
- the contact point where more information can be obtained;
- the approximate number of data subjects and number of personal data records concerned;
- the (currently known and/or anticipated) consequences thereof;
- the (proposed) solution;
- the measures that have already been taken.

8. Requests from data subjects

8.1 We shall promptly notify you of any request we have received from a data subject. You shall then be responsible for properly handling the request. We may notify the data subjects of the fact that their requests have been forwarded and will be handled by you.

8.2 When necessary, we shall assist you in fulfilling your obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing.

9. Non-disclosure and confidentiality

9.1 All personal data received by us from you within the framework of this Data Processing Agreement is subject to a duty of confidentiality. With regards to sub-processors engaged within the scope of this Data Processing Agreement or other providers of professional services, exchanging the confidential personal data is only allowed if such sub-processor or third party is also legally bound to a similar obligation of confidentiality.

9.2 This duty of confidentiality will not apply if you (i) have expressly authorized the provision of such information to third parties, (ii) where the provision of the information to third parties is reasonably necessary taking into account the nature of the instructions and the implementation of this Data

Processing Agreement, or (iii) if there is a statutory obligation to provide the information to a third party.

10. Audit

10.1 In order to confirm compliance with all points in this Data Processing Agreement, and article 28 of the GDPR when applicable, you shall be entitled to have audits carried out. You may choose to conduct the audit by yourself or mandate an independent auditor who is bound to confidentiality. The costs of the audit will be borne by you.

10.2 The audit will only take place after you have requested and assessed similar audit reports made available by us and provide reasonable arguments to conduct an audit. Such an audit is justified when the audit reports provided by us give no or insufficient information regarding our compliance with this Data Processing Agreement. The audit initiated by you will take place no more than once a year and only after you have provided two weeks prior notification.

10.3 We will cooperate with the audit and will make available any reasonably necessary information, including supporting information such as system logs and employees as timely as possible.

10.4 The findings in respect of the performed audit will be discussed and evaluated by the Parties and, where applicable, implemented by us.

11. Duration and termination

11.1 This Data Processing Agreement is entered for the duration set out in the agreement between you and us. If no clear term has been agreed upon, then this Data Processing Agreement will apply as long as we process personal data on your behalf. If we no longer process personal data on your behalf, then this Data Processing Agreement is automatically terminated.

11.2 This Data Processing Agreement cannot be terminated unilaterally by either Party if such termination would lead to non-compliance with applicable privacy legislation.

11.3 Upon termination of the Data Processing Agreement, the Parties shall discuss and agree if any personal data still in our systems should be deleted or returned to you.

11.4 Parties shall provide their full cooperation in amending this Data Processing Agreement insofar necessary because of any amended privacy laws and regulations.

12. Miscellaneous

12.1 This Data Processing Agreement forms an integral part of the agreement between you and us. All rights and obligations under our Terms of Use, including the limitations on liability and applicable law, apply mutatis mutandis to this Data Processing Agreement.

12.2 In case of a dispute between a data subject and one of the parties as regards to compliance with these terms, that party shall use its best efforts to resolve the issue amicably in a timely fashion. The parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

12.3 These terms shall be governed by Dutch law. The parties shall try to solve any dispute between them amicably. In case either party wishes to take a dispute to court, then such dispute shall exclusively to the competent court in the district of Oost-Brabant location 's-Hertogenbosch.

Appendix II

Technical and Organizational Measures

Hereunder you will find a description of the technical and organizational measures implemented by us (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Infrastructure security

Server Network
The IXON Cloud is a complex network of over 150 servers, distributed globally among various hosting providers. All are situated in data centers maintaining the highest security standards.

High Availability
Most IXON servers are set up for high availability or have redundant deployments, ensuring that a single hardware or network failure won't compromise the IXON Cloud's availability.

Backups
Stateful servers are backed up weekly. Additionally, backups for essential customer and machine data are created every four hours. These backups are monitored in real-time for accuracy and undergo monthly validity tests.

Server Access
Only senior IXON personnel, including developers and administrators, can access servers. This is facilitated through unique usernames and private SSH keys. All server-related activities are logged and audited.

Real-time Monitoring
Servers are constantly monitored using an array of both standard and custom checks analyzing internal metrics. Any deviations or anomalies immediately alert relevant staff.

Server Configuration
A master node manages server configuration, guaranteeing uniformity across servers. This system also enables effortless deployment of new servers.

Server Hardening
Our servers undergo a hardening process, minimizing vulnerabilities by eliminating unused protocols, tightening file access permissions, and mandating robust passwords.

Patch Management
Critical patches are applied within a day. Weekly, non-critical software patches are assessed and those enhancing uptime, performance, or security are deployed.

Firewalls
Each server boasts a firewall, adopting a deny-all, permit-by-exception approach. Exceptions are rigorously evaluated to be as strict as possible, employing methods like source IP or protocol whitelisting.

Inter-server Exchange
IXON Cloud servers operate within an internal mesh network, ensuring that communications between servers never traverse the public Internet.

Data Privacy and confidentiality

Privacy by Design
Every change in data handling, from software updates to subcontractor shifts or internal process modifications, undergoes a privacy impact analysis to ensure data privacy.

GDPR Compliance
Personally identifiable information (PII) is processed and stored by EU-based third parties in line with GDPR legislation, as detailed in Part V. IXON has designated a privacy officer to ensure compliance.

Data Ownership
All personal and machine data stored or created in the IXON Cloud belongs to the user. IXON may not, in any shape or form, misuse, distribute or sell this information.

Data Retention
Data does not expire as long as you have an active user account. After deleting your account, data may be deleted after three months.

TLS Encryption
HTTPS and MQTT connections use TLS 1.2 or higher for encryption. We permit only "strong" encryption algorithms that support perfect forward secrecy, utilizing RSA keys of 4096 bytes.

VPN Encryption
VPN connections utilize single-use VPN certificates and are encrypted using AES-256-CBC with SHA512.

Password Hashing
IXON Cloud passwords are stored as hashes using Argon2id, configured with 3 iterations, 4 degrees of parallelism, 64 MiB memory, and a 16-byte salt.

Vulnerability management

Vulnerability scanning
IXON Cloud servers are tested for vulnerabilities every week using both internal and external scans.

Penetration Testing
Each year, the IXON Cloud and IXrouter undergo 2 to 3 third-party penetration tests. Tests range from black box evaluations of the entire IXON Cloud to white box analyses of significant architectural changes.

Log analysis
All server logs are gathered in a centralized log system and automatically analyzed according to community-maintained and custom security rules..

Incident handling

Security Breach Protocol

A protocol is in place to address security incidents effectively and efficiently. This protocol involves the following steps: 1) Incident verification, 2) Containment, 3) Evaluation, and 4) Lessons learned.

Incident Notification
Impacted parties and users are notified promptly about a security incident via email. We strive to be as transparent as possible in our communication.

Incident Training
Annually, using a tabletop setting or a simulated environment, we replicate a major security breach to ensure IXON personnel are familiar with their role in the security breach protocol.

Business Continuity Plan
A plan is in place to ensure business operations continue smoothly during various man-made or natural events.

Application Security

Authentication
The initial login to the IXON Cloud uses Basic Authentication. After successful login, users receive a Bearer token valid for their session duration.

Password strength
We don't enforce traditional complexity requirements for passwords. Instead, we mandate passwords be deemed "unguessable" (no. guesses > 10^8) by our strength estimator. This system also blocks commonly used passwords.

Brute force protection
Repeated failed login attempts (>10 tries) result in a temporary block. This time increases with subsequent failed attempts, up to a maximum of 1 hour.

Multi-factor authentication
Time-based one-time passwords (TOTPs) can be employed as an additional authentication factor. They can be activated for individual users or mandated for all users within your IXON Cloud environment.

Granular permission
Administrators can fine-tune permissions using user groups and roles, adjusting access for multiple users simultaneously. These permissions can provide access to all devices, target specific ones, or restrict certain device services, such as VNC, VPN, or HTTPS.

Logical separation of data
Although customer data resides in multi-tenant environments, we implement multiple layers to safeguard data confidentiality. Initially, requests validate your Bearer Token. Subsequently, data filtering occurs based on your domain, company ID, and permission role – returning only the information you're authorized to view.

Session control
Active IXON Cloud sessions are accessible within your account details. Implementing a security change, like updating your password, auto-revokes all ongoing sessions.

Audit trails
The IXON Cloud provides device-specific and company-wide audit trails, offering users a comprehensive record of historical events.

Software development

Security by design
Security requirements are created prior to development which must be met before changes may be deployed.

Peer reviews
Any code modifications undergo a review by at least one senior, independent developer. This ensures readability, clarity, and completeness. All identified issues must be resolved before approval.

Automated testing
Upon committing changes to our software versioning system, the code undergoes comprehensive automated tests. This encompasses unit tests, scenario tests, and security evaluations.

Staged deployment
We employ distinct environments to segregate (potentially) insecure code before it reaches production:

- Development: Runs locally on developers' systems, facilitating code modifications.
- Testing: Houses finished features and serves as a platform for manual tests.
- Staging: Contains code ready for production, and is utilized for integration and stress testing.

Organizational security

Vendor reviews
Suppliers and third parties undergo an initial security review and subsequent annual checks. Essential suppliers, like hosting providers, are mandated to possess an ISO27001 certificate or equivalent.

Training and awareness
All security personnel must meet a set training quota each quarter. New hires are trained on IXON's security policies during onboarding, and the entire staff regularly undergoes updates on pertinent security subjects.

Policy management
Our security policies are accessible via an internal webpage. Policy alterations are documented, requiring approval before being published. Policies undergo a biannual review.

Risk management
Quarterly risk assessments categorize threats by likelihood and impact. Risks exceeding acceptable thresholds are documented in a treatment plan, outlining specific corrective actions and their respective deadlines.

Endpoint protection
All company hardware features hard-disk encryption and endpoint protection software. In-depth antivirus scans run weekly, with any anomalies instantly reported to our security team.

Certification
IXON's management system holds certifications in:

- ISO9001 - Quality management
- ISO27001 - Information security management
- ISO27017 - Cloud System Information Security
- ISO27701 - Privacy management

Accredited third-party NCI conducts yearly external audits.

Internal audits
Every quarter, internal audits are undertaken by independent IXON employees.

Appendix III

List of sub-processors

Company	Database location	Type of data stored	Website
Digital Ocean LLC	The Netherlands	Audit trail data	digitalocean.com
		Customer data	
		Machine data (Backup)	
UpCloud Ltd.	The Netherlands	Audit trail data	upcloud.com
ElasticCloud	Centralized logging	The Netherlands	elastic.co/cloud
Mailchimp	Email services	United States	mailchimp.com
TransIP	Customer data backup	The Netherlands	www.transip.eu
Hubspot	Corporate website (www.ixon.cloud) and integration with CRM	Germany	hubspot.com
Salesforce.com Inc.	CRM	France and Germany	salesforce.com