DATA PROCESSING AGREEMENT

This Data Processing Agreement, including the Appendices attached hereto ("the DPA") is hereby entered into by and between:
Signatory company ("The Customer", "the Data Controller")
InfraCom Communications AB, corporate registration number, Gamlestadsvägen 1, 415 11 Göteborg, Sweden ("InfraCom Communications", "the Data Processor")
Each of the Data Controller and the Data Processor is referred to as a "Party" and together as the "Parties".

1. DEFINITIONS

1.1. To the extent that the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the "General Data Protection Regulation", "GDPR"), contains terms equivalent to those used in the Agreement, such terms shall be interpreted and applied in accordance with the GDPR.

1.2. InfraCom Communications offers a cloud based communication platform Infinity. Subject to the terms of the Agreement, InfraCom Communications will provide The Customer access to the platform for use of agreed services, as specified in the Agreement (below the "Services").

1.3. Applicable Data Protection Legislation refers to the General Data Protection Regulation (GDPR), regulations and practices relating to the General Data Protection Regulation, national supplementary legislation to the General Data Protection Regulation including the Swedish Data Protection Act, provisions, and opinions issued by supervisory authorities, including the European Data Protection Board (EDPB), and the Commission's legal acts concerning personal data.

1.4. Confidential information refers to all information related to or connected with this DPA and the processing of personal data under this DPA, as well as any other information obtained by a Party in its capacity as a Party to this DPA, regardless of the form or medium in which such information was received, or whether the information is provided orally or in writing. Confidential Information does not include information that: i) was already known to the Party at the time of receipt, provided the Party can substantiate this with written documentation, ii) was already publicly available at the time of entering into this DPA, or becomes publicly available during the term of this DPA, other than as a through a breach of this DPA, iii) was received from a third party, provided the Party can substantiate that the third party did not obtain the information, directly or indirectly, from the Party, iv) was created or developed independently by the Party, without reference to the Confidential Information received from the other Party, v) was disclosed by the Party without restrictions on further dissemination, provided the Party can substantiate this with written documentation, or vi) is required to be disclosed by law, or by order from a competent authority or court, but only after notifying the affected Parties of the required disclosure.

2. AGREEMENT DOCUMENTS, PRECEDENCE AND PURPOSE

2.1. The Parties have entered into a services agreement including appendices for The Customer's use of the InfraCom Communications platform and other Services (the "Services Agreement"). InfraCom Communications will process personal data on behalf of The Customer in connection with provisioning of Services under the Services Agreement. This DPA applies in relation to the to the Services Agreement. The clauses of this DPA are applicable to the processing of personal data in accordance with Appendix 1. Appendix 1-2 are attached hereto and form an integral part of the clauses in this DPA as set out below.

- Appendix 1 – Personal data and processing
- Appendix 2 – Security measures
- Appendix 3 – List of Sub-processors

2.2. In the event of any conflict or discrepancy between the provisions of this DPA and the Services Agreement, as well as any other agreements between the Parties existing at the time these clauses are agreed upon or subsequently entered into, the provisions of this DPA shall prevail.

2.3. InfraCom Communications has, through this DPA, undertaken to process personal data on behalf of The Customer in conjunction with the Services. The Parties have agreed to regulate the scope and the details of the processing through the establishment of this DPA in accordance with article 28 GDPR (specifically Article 28.3) of the GDPR, to ensure the protection of the rights of the Data Subjects.

3. RESPONSIBILITIES AND INSTRUCTIONS

3.1. The Customer shall be responsible for ensuring that all processing of personal data is legal and is carried in accordance with this DPA and Applicable Data Protection Legislation. The Customer shall, amongst others, be responsible for ensuring that the processing of personal data performed by InfraCom Communications on behalf of the Customer has a legal basis.

3.2. The Customer shall provide InfraCom Communications with the information and personal data that are necessary and appropriate for the Customer to be able to fulfill its obligations in accordance with this DPA and Applicable Data Protection Legislation.

3.3. The Customer shall only process the personal data that is adequate and relevant for the specifically chosen purpose of the processing and shall only grant InfraCom Communications access to the personal data that is necessary for the purpose of the processing. This obligation applies, for instance, to the volume of personal data, the duration of processing and the accessibility of the personal data.

3.4. The Customer (on behalf of Additional Controllers where relevant) is responsible for the processing of all personal data which InfraCom Communications processes on behalf of The Customer and Additional Controllers for the purpose of providing the Services.

3.5. The Customer is responsible for providing InfraCom Communications with documented instructions. InfraCom Communications shall process the personal data only on the documented instructions from The Customer. The documented instructions shall, among other things, but not exclusively, regulate the purpose of the processing, the categories of personal data to be processed, the categories of data subjects whose personal data is processed, the nature and the duration of the processing. The documented instructions are specified in Appendix 1 ("Included Personal Data").

3.6. InfraCom Communications undertakes to only process the Included Personal Data in accordance with the controller's written instructions as set in this DPA, and only to the extent necessary for the performance of the Services Agreement. For the avoidance of doubt, the DPA and the Services Agreement include exhaustive instructions to InfraCom Communications as of the signing date. InfraCom Communications may alternatively terminate the DPA in such circumstances, subject to section 13.2 below.

3.7. If InfraCom Communications lacks instructions that it deems necessary to perform its tasks, InfraCom Communications shall, without undue delay, inform the Customer in writing and await the necessary instructions.

3.8. InfraCom Communications shall immediately inform The Customer if, in InfraCom Communications's opinion, an instruction infringes Applicable Data Protection Legislation.

3.9. InfraCom Communications shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. InfraCom Communications is responsible for restricting access to personal data and shall therefore ensure that no more persons than necessary have access to the personal data.

3.10. InfraCom Communications shall provide reasonable assistance to The Customer in ensuring compliance with the obligations set out in Applicable Data Protection Legislation with regard to security for processing, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject, data protection impact assessment and prior consultation, taking into account the nature of processing and the information available to InfraCom Communications.

3.11. Taking into account the nature of the processing, InfraCom Communications shall assist The Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of The Customers´ obligation to respond to requests for exercising the data subject's rights laid down in Applicable Data Protection Legislation.

3.12. The Customer is responsible for safeguarding the data subject's rights and responding to the data subject's requests for exercising its data subject's rights laid down in Chapter III GDPR, such as right to information, access to personal data, rectification, erasure and right to restrict the processing of personal data. If the data subject's request to exercise its data subject's rights is addressed directly to InfraCom Communications, InfraCom Communications shall inform The Customer without undue delay, upon The Customer is responsible for replying to the data subjects request, unless otherwise have agreed in

writing between the Partiers. InfraCom Communications furthermore undertakes to reasonably assist The Customer in fulfilling the data subject's rights.

3.13. The Customer acknowledges that the Services include functionality to enable The Customer to retrieve information and access personal data from the Services independently from InfraCom Communications, in order for The Customer to answer data subject requests and/or take other actions required pursuant to Applicable Data Protection Legislation. If and to the extent The Customer requests InfraCom Communications to assist on a matter which The Customer could have handled itself through the Services, then InfraCom Communications is entitled to reasonable compensation for any and all such assistance or information provided.

3.14. In the event that InfraCom Communications receives a request from a governmental authority or other law enforcement entity seeking access to Included Personal Data, InfraCom Communications shall, unless legally prohibited, promptly notify The Customer and provide all pertinent details regarding the request. InfraCom Communications shall cooperate with The Customer in challenging or limiting the scope of such requests where appropriate under Applicable Data Protection Legislation. The Customer retains the right to direct the response to any such request.

3.15. In the event of a request by data subjects, supervisory authorities, or any other third party, regarding the processing of the Included Personal Data, the Parties shall cooperate and exchange information to a necessary extent.

3.16. InfraCom Communications shall, when necessary and upon request, assist The Customer in fulfilling its obligations arising from the provisions of the General Data Protection Regulation regarding the performance of data protection impact assessments and prior consultations with the supervisory authority.

3.17. InfraCom Communications shall maintain a record of all categories of processing activities carried out on behalf of The Customer, containing:

- The name and contact details of the processor and of the controller on behalf of which the processor is acting, and, where applicable, of the processor's or of the controller´s representative and the Data Protection Officer,
- The categories of processing carried out on behalf of each controller,
- Where applicable, transfers of personal data to a third country or an international organization, including the identification of the third country or the international organization and documentation of suitable safeguards,
- Where possible, a general description of the technical and organizational security measures.

This record shall be in writing, including in electronic form.

4. CONFIDENTIALITY

4.1. Each Party undertakes, during the term of the agreement and thereafter, not to, without the other Party´s prior written consent, disclose or reveal to any third party personal data or information about the other Party's business that is reasonably deemed to be

regarded as trade secrets, and hence "Confidential Information". Information which a Party has stated to be confidential is always considered as trade secrets.

4.2. The confidentiality requirement does not apply to information which a Party can show has been known to him in another way than in connection with the assignment or public knowledge.

4.3. The confidentiality requirement does further not apply when a Party is required by law or court order to disclose information. If a Party were to have or be required to disclose such information, that Party undertakes to immediately notify the other Party. The disclosing Party shall use its best efforts to ensure that the information disclosed in accordance with this clause is, to the greatest extent possible, treated confidentially by the recipient of the information.

4.4. The Parties undertake to use the Confidential Information solely for the purpose of fulfilling their obligations under the Services Agreement and this DPA and not for any other purpose.

4.5. Each Party is responsible for ensuring that its employees, subcontractors and subcontractors' employees are subject to confidentiality in accordance with section 5.1 above, and that such persons only have access to information to the extent which is necessary to perform their obligations.

5. SECURITY

5.1. InfraCom Communications guarantees that it possesses the necessary technical and organizational capacity and ability to fulfill its obligations under this DPA and the Applicable Data Protection Legislation.

5.2. InfraCom Communications shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including but not limited to pseudonymisation and encryption of personal data, ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems, and regularly testing, assessing, and evaluating the effectiveness of such measures in line with GDPR Article 32.

5.3. The security measures are described in Appendix 2.

5.4. InfraCom Communications undertakes to provide The Customer with prior written notice of any intention to modify the manner in which personal data is processed or to implement other changes that could reasonably be expected to affect the security of the data subjects, the rights of the data subjects, compliance with this DPA, or Applicable Data Protection Legislation. Such notice shall be provided in writing at least thirty (30) days before the planned change and shall include a detailed description of the proposed changes as well as their potential impact on processing security, the rights of the data subjects, and compliance with this DPA and Applicable Data Protection Legislation. InfraCom Communications shall obtain the Customers prior written consent before implementing any changes as described above. If such written consent is not provided within the agreed

timeframe, the changes shall not be implemented. In the event of any disagreement regarding the proposed changes, the Parties shall promptly engage in discussions to reach a mutually acceptable solution. Until such a solution is reached, the original processing of personal data shall remain unchanged.

6. PERSONAL DATA BREACHES

6.1. In the event that InfraCom Communications suspects or becomes aware of a personal data breach, InfraCom Communications must immediately, but under no circumstances later than 24 hours after such suspicion or knowledge has arisen, notify The Customer of the suspected or ascertained personal data breach and otherwise provide The Customer with the necessary assistance in order to make it possible for The Customer to fulfil its obligations according to data protection legislation.

6.2. In the event of a suspected or discovered personal data breach, InfraCom Communications shall investigate the breach immediately and take appropriate measures to mitigate its potential negative effects.

6.3. The Customer shall be provided with a description of the personal data breach. Such description shall contain at least:

- a description of the type of personal data breach, including where possible the categories of and the approximate number of data subjects concerned, as well as the categories of and approximate number of personal data items concerned,
- the name of and contact details for the Data Protection Officer or other contact points from where further information may be obtained,
- a description of the likely consequences of the personal data breach, and
- a description of the measures that have been taken or proposed by InfraCom Communications to remedy the personal data breach, including, where appropriate, measures to mitigate its potential negative effects.

If it is not possible to provide the information at the same time, the information may be provided in stages without further unnecessary delay.

6.4. A notification in accordance with the above shall contain all the information The Customer needs to fulfil its obligations towards the supervisory authority.

6.5. InfraCom Communications shall assist The Customer in ensuring that The Customers´ obligations concerning personal data breaches are met, taking account of the type of processing and the information that InfraCom Communications has access to.

6.6. InfraCom Communications undertakes to document all personal data breaches, including suspected personal data breaches and the circumstances surrounding the personal data breach, its effects and the corrective measures taken and of which InfraCom Communications is aware of. Upon request, the documentation shall be provided to The Customer as soon as possible.

6.7. For the avoidance of doubt, InfraCom Communications will not be entitled to compensation for assistance related to a personal data breach caused by InfraCom Communications.

7. SUB-PROCESSORS

7.1. InfraCom Communications may engage a Sub-processor only if specific prior written authorization has been obtained from the Customer. The Parties agree that such specific prior written authorization is provided in Appendix 3. The Parties shall keep Appendix 3 updated.
InfraCom communications is a telecom operator in many jurisdictions and all telecom operator InfraCom communication use in interconnections is not seen as a Sub-processor. These operators will thus not be included in Appendix 3 if they are used for interconnect without handling any personal data.

7.2. If specific prior written authorization has been provided by The Customer in accordance with this DPA, as specified in an updated version of Appendix 3, InfraCom Communications shall notify The Customer in writing of any plans to engage a new Sub-Processor or replace an existing Sub-Processor. This is intended to provide The Customer the opportunity to raise any objections to such changes.

7.3. InfraCom Communications shall enter into data processing agreements with all its Sub-processors that will process Included personal data. Such data processing agreement shall impose the corresponding obligations to those of InfraCom Communications under this DPA on the Sub-Processor, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in accordance with the requirements of Applicable Data Protection Legislation. InfraCom Communications will never store any personal data outside of EU.

7.4. InfraCom Communications and the Sub-processor shall agree on a third-party beneficiary clause, under which The Customer – in the event that InfraCom Communications ceases to exist in a factual or legal sense, or becomes insolvent – shall have the right to terminate the Sub-processors data processing agreement and instruct the Sub-processor to delete or return the personal data.

7.5. InfraCom Communications shall be fully liable to The Customer for the performance of the Sub-processors' obligations according to the DPA and corresponding sections in any data processing agreements.

8. AUDIT

8.1. Customer has the right to, on its own or through an auditor, within reasonable extent and prior notice to InfraCom Communications, undertake an audit, including inspections, of InfraCom Communications. Such third-party auditor must execute a written confidentiality agreement acceptable to InfraCom Communications before conducting the audit. Subject to Section 3.5 above, InfraCom Communications will to a reasonable extent assist and permit audits by Additional Controllers and supervisory authorities. InfraCom Communications is entitled to reasonable compensation thereof.

8.2. The Customer acknowledges that InfraCom Communications may engage third party cloud providers to provide the Services. Any audit or inspection of such third-party cloud provider is subject to the policies and rules implemented by such third-party cloud provider from time to time.

8.3. To request an audit, Customer must submit a detailed audit plan to InfraCom Communications at least ten (10) business days in advance of the proposed audit. The audit plan must describe the proposed scope, duration, and start date of the audit. InfraCom Communications will review the audit plan and provide The Customer with any concerns or questions. Parties shall negotiate in good faith in agreeing on a final audit plan.

8.4. InfraCom Communications must, upon The Customer's request and to a reasonable extent, provide The Customer available information about the processing of the Included Personal Data, in order to demonstrate compliance with its obligations under Applicable Data Protection Legislation. InfraCom Communications shall have the right to reasonable compensation thereof.

8.5. The Customer shall document the results of the audit and delete it when it is no longer necessary for the purpose of the audit.

9. TRANSFERS TO THIRD COUNTRIES

9.1. InfraCom Communications will not transfer the Included Personal Data outside of the EU/EEA.

9.2. Notwithstanding any expectations to the contrary, if a transfer of personal data is to take place InfraCom Communications shall prior to this transfer obtain written consent from The Customer. A transfer to a third country also requires that InfraCom Communications, before initiating such a transfer, complies with the requirements and measures set out in Chapter V of the GDPR regarding third country transfers. This includes, among other things, appropriate safeguards such as the European Commission-approved Standard Contractual Clauses (SCC) or other approved exceptions, including but not limited to for the performance of a contract or obtaining explicit consent from the data subject.

10. LIABILITY FOR DAMAGES

10.1. InfraCom Communications shall indemnify The Customer for any damage suffered by The Customer, the data subjects, or any other natural or legal person or authority as a result of InfraCom Communications's processing of personal data in violation of the documented instructions (including deficiencies in security measures) (Included Personal Data), This DPA, or Applicable Data Protection Legislation.

10.2. The Customer shall indemnify and hold InfraCom Communications harmless for any damages suffered by InfraCom Communications and for any claims directed against InfraCom Communications that arise from or are related to InfraCom Communications's processing of personal data in accordance with the instructions from The Customer or otherwise in accordance with this DPA. Any claims or demands may only be made in relation

to personal data that needs to be processed to fulfill the Services Agreement in accordance with this DPA.

10.3. The Parties agree that if one Party is held liable under this clause, the Party that has paid compensation shall be entitled to recover from the other Party the portion of the compensation corresponding to the other Party's liability for the damage, in accordance with Article 82 of the GDPR.

10.4. Any limitation of liability in any other agreement between the Parties shall not apply in relation to processing covered by this DPA.

11. TERM AND TERMINATION

11.1. This DPA shall enter into force on the date when authorized representatives of both Parties have signed the DPA and shall remain valid for as long as the Services Agreement between the Parties is in effect ("Term of the Agreement").

11.2. This DPA remains in effect as long InfraCom Communications processes include personal data on behalf of The Customer and Additional Controllers.

11.3. If the Services Agreement is terminated and a new agreement of the same kind is entered into without a new Data Processing Agreement being concluded, this DPA shall also apply to the new Services Agreement. This Agreement shall remain in effect even if the Service Agreement ceases and shall continue until InfraCom Communications and any Sub-processors engaged by InfraCom Communications have ceased processing personal Data on behalf of The Customer.

12. OBLIGATIONS AFTER THE TERMINATION OF THE AGREEMENT

12.1. Upon termination, all The Customer data shall be deleted within thirty (30) days, unless otherwise agreed upon in writing or storage of the data is required according to the law by which InfraCom Communications is governed. If The Customer requires assistance in relation to export of data, InfraCom Communications shall be entitled to adequate compensation thereof.

12.2. If and to the extent required by Union or national law that InfraCom Communications shall store the Included Personal Data, InfraCom Communications has the right to do so notwithstanding what has been stated above.

13. MODIFICATIONS / AMENDMENTS

13.1. Any modifications or amendments to this DPA, including those required as a result of changes in Applicable Data Protection Legislation or regulatory guidance, shall be made in writing, agreed upon by both parties and signed by duly authorized representatives of both Parties. Upon receiving written notice of a proposed change from either party, the parties shall engage in good faith negotiations to reach a mutually acceptable amendment. Until

such an amendment is executed, the existing terms of this DPA shall remain in full force and effect.

14. ASSIGNMENT

14.1. Neither Party is entitled to transfer, in whole or in part, its obligations or rights under this DPA to a third party without prior written approval from the other Party.

15. NOTICES

15.1. Notices, requests for personal data, and communications under this DPA shall be made in writing. Notices shall be addressed to the contact persons specified below.
The Data Controller
[Company Name]
[name of contact person], [e-mail contact person]
The Data Processor
InfraCom Communications AB
Data Protection Officer, dpo.icc@infracom.se
InfraCom Communications has appointed the above dedicated Data Protection Officer responsible for overseeing our data protection strategies, conducting regular compliance audits, and managing data subject requests. The DPO also serves as our primary liaison with regulatory authorities.

16. GOVERNING LAW AND DISPUTES

16.1. This Agreement shall be interpreted and governed by Swedish law.

16.2. Any dispute, controversy or claim arising out of or in connection with this Agreement, or the breach, termination or invalidity thereof, shall be finally settled by arbitration in accordance with the with the Rules for Expedited Arbitrations of the SCC Arbitration Institute. The seat of arbitration shall be the Stockholm Chamber of Commerce Arbitration Institute. The language to be used in the arbitral proceedings shall be Swedish. This Agreement shall be governed by the substantive law of Sweden.

Appendix 1 to the DPA

Personal data and processing

The following documents constitute the documented instruction together with Appendix 2. Definitions used in this Appendix 1 shall have the same meaning as in the DPA unless the context clearly indicates otherwise.
This Appendix 1 sets out the details concerning the Included Personal Data and processing thereof pursuant to the DPA.
The purpose of this Appendix 1 is to clarify which processing and personal data that is covered by the DPA, and to fulfill the requirements of the Applicable Data Protection Legislation regarding the obligation to specify the categories of a processor's processing of personal data.

The subject, nature, and the purpose of processing under the DPA

Infinity is a PBX cloud solution with call, message and AI capabilities

Endpoint connected to Infinity is defined as

- Mobile phones where InfraCom Communications is the Operator
- Any SIP device connected to Infinity SIP servers
- Calls from mobile phones that are interconnected through MEX to Infinity
- All communications from Infinity clients (Mobile app and Desktop app)
- External API connections to Infinity API

Data is processed during communication and interaction with customers using any endpoint connected to Infinity.
Data is processed during account/user registration and management in the Infinity clients.
Calls and text that are sent to an external interconnect telecom connection are not seen as personal data to a sub-processor and that sub-processor is not included in annex 3.

Duration of the data processing

Personal data is saved for 12 months by default. This can be changed in settings in the Infinity portal by The Customer and different data can have different retention period. InfraCom Communications are regulated by the telecom laws in different EU countries and will in case it is regulated save data according to the rules from regulators.

InfraCom Communications will process Personal Data solely for the period during which the Services are provided under the Services Agreement, including any additional period needed for invoice or regulated demands or required by applicable law. Upon termination or expiration of the Services Agreement, personal data will be returned or, where technically feasible, securely deleted in accordance with InfraCom Communication's retention policies and legal obligations.

The categories of personal data

InfraCom Communications processes personal data as part of delivering its services. The specific categories of personal data include, but are not limited to:

- **Customer Data:** Information provided by The Customer during account setup and subsequent interactions (e.g., account details, transactional records).
- **Behavioral Data:** Data generated from user interactions, such as engagement metrics, and data that support the optimization of support, operational, marketing and sales efforts. Behavioral data may include, but is not limited to call detail records including different queue data, recordings of conversations, transcriptions from conversations, insights from processes transcriptions, meeting data such as meeting time and participant engagement.

The categories of data subjects

The determination of which individuals' personal data is processed rests with The Customer and its authorized Users. Accordingly, InfraCom Communications processes personal data for the following categories of data subjects:

- **Customer Contacts:** Individuals whose details are provided by The Customer, data may include, but is not limited first name, last name, address, phone number, email, and country of residence.
- **Communication Participants:** Individuals whose participation in video, audio or text communication results in the capture of recordings and associated metadata.

Processing activities

In alignment with the Services Agreement, InfraCom Communications undertakes the following detailed activities concerning the Included Personal Data, which may include, but is not limited to:

- **Call and Messages Management:** Utilizing personal data during calls, meetings and messaging that the clients may share and handling any post data processing requirements.
- **Data Analysis:** Conducting in-depth analysis and generating statistics related to client communications.
- **API Integration:** Establishing connections and enriching data between our platform and the client's Customer Relationship Management (CRM) and other internal systems.

Appendix 2 to the DPA

Security measures

The following documents constitute the documented instruction together with Appendix 1. Definitions used in this Appendix 1 shall have the same meaning as in the DPA unless the context clearly indicates otherwise.
At InfraCom Communications, safeguarding personal data is a top priority. Our security framework is designed to ensure compliance with the General Data Protection Regulation (GDPR) while maintaining the confidentiality, integrity, and availability of personal data processed in our EU-based cloud service. We achieve this through a layered approach that integrates robust technical controls with rigorous organizational policies.

1. Data Protection Officer (DPO)

InfraCom Communications has appointed a dedicated Data Protection Officer responsible for overseeing our data protection strategies, conducting regular compliance audits, and managing data subject requests. The DPO also serves as our primary liaison with regulatory authorities. For any data protection inquiries, please contact: dpo.icc@infracom.se.

2. Data encryption

- **Data in Transit:** We secure all data transmitted over our networks using TLS 1.2/1.3 protocols to prevent interception and unauthorized access.
- **Data at Rest:** Sensitive data is encrypted using AES-256.

3. Secure development practices

We maintain a robust security posture from the earliest stages of development by integrating a comprehensive suite of security tools directly into our CI/CD pipelines.
Our pipelines include:

- **Static Application Security Testing (SAST):** Scanning our codebases to identify potential vulnerabilities early in the development process.
- **Interactive Application Security Testing (IAST):** Continuously monitoring running applications to detect vulnerabilities in real time.
- **Software Composition Analysis (SCA):** Analyzing third-party components to manage and mitigate risks associated with open-source software.

4. By embedding these automated security measures into our development lifecycle

We proactively address potential risks and ensure that security remains a foundational element of our software delivery process.

5. Access control

The Data Processor implements zero trust network access, replacing traditional VPN infrastructure. All access to internal resources requires identity verification and device posture checks through a secure client application.
We enforce role-based access control (RBAC) and implement multi-factor authentication (MFA) to ensure that only authorized personnel can access sensitive data.
Access rights are assigned based on the principle of least privilege and are reviewed periodically.
Comprehensive logging and monitoring mechanisms are in place to detect and respond to any unauthorized access attempts.

6. Data backup and recovery

Regular backups are performed daily and stored securely in geographically diverse locations to safeguard against data loss.
Our backup strategy is underpinned by clearly defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
We conduct periodic disaster recovery drills to ensure rapid restoration of data and continuity of service in the event of an incident.

7. Network security

Our network infrastructure is protected by industry-leading firewalls, intrusion detection/prevention systems (IDS/IPS), and strategic network segmentation.
We perform regular vulnerability assessments and penetration tests to proactively identify and mitigate potential security weaknesses.

8. Regular updates and patch management

A robust patch management process ensures that all software and systems are kept up to date.
Critical updates are tested and deployed promptly to address any vulnerabilities.

An up-to-date inventory of software and systems supports comprehensive and timely patching across the infrastructure.

9. Employee training and awareness

All employees receive regular training on data protection, security best practices, and GDPR compliance.
Training programs include periodic refresher courses and simulated phishing exercises to maintain a high level of security awareness.
We assess training outcomes continuously, ensuring that our team remains informed about evolving threats and compliance requirements.

10. Data Protection Impact Assessments (DPIAs)

Prior to introducing new processing activities or making significant changes, we conduct DPIAs to identify and mitigate potential risks to personal data.
DPIAs are thoroughly documented and reviewed periodically, ensuring that risk management remains an ongoing process.

11. Incident response and monitoring

InfraCom Communications maintains a comprehensive incident response plan that outlines clear procedures for detecting, containing, and mitigating security incidents.
We employ a Security Information and Event Management (SIEM) system for centralized logging and real-time monitoring, enabling rapid identification and response to anomalies.
By integrating these measures, we demonstrate a strong commitment to data protection and regulatory compliance. Our security practices are continuously reviewed and enhanced to stay ahead of emerging threats and ensure the ongoing safety of personal data entrusted to us.

12. Security and Data Protection Policies

- **Device Security:** Workstations shall automatically lock after 5 minutes of inactivity. Re-authentication is required to regain access.
- **Data Destruction:** Employees must use secure erasure methods for personal data on devices, ensuring data cannot be recovered through standard recovery tools or forensic methods.
- **Visitor Management:** All visitors must be escorted by authorized personnel at all times within company premises. Visitor access logs are maintained.

Appendix 3 to the DPA

Sub-processors

Below is a list of the Sub-processors engaged for the processing of personal data under this DPA.
The list shall be amended and updated each time a new Sub-processor is engaged, or a Sub-processor is replaced throughout the term of this DPA.
The Customer (The Data Controller) has approved the use of the following Sub-processors:

Name of the Sub-processor	Registration number	Description of services	Location
InfraCom Managed Services AB	5562-650274	Hosting services	Gothenburg, Sweden
Telenor Sverige AB	556421-0309	MVNO provider	Sweden
Microsoft Corporation	One Microsoft Way, Redmond, WA 98052, USA	Azure, Microsoft 365, Used when activating services like AI, O365 syncing	EU/EES,
Google Cloud Platform (Google LLC)	Google Dublin Campus, Grange Castle Business Park, 22 Baldonnel Rd, Dublin 22, D22 X602, Ireland	Cloud infrastructure, storage, and related services, May by used when activating service like AI, google cloud syncing	EU/EES
Amazon Web Services (AWS)	Amazon AWS FRA54, Eschborner Landstraße 100, 60489 Frankfurt am Main, Germany	May be used for services in UK or AI	EU/EES