Data Processing Agreement

This Data Processing Agreement including the Annexes (the "**DPA**") is part of the Agreement between Customer and Incision Group B.V. ("**Incision**"), unless otherwise stated on your Order Form. All capitalized terms not defined in this DPA shall have the meaning given to them in other parts of the Agreement or in art. 4 of the GDPR.

Whereas:

- the Customer has requested certain Services from Incision as defined in the Agreement;
- with regard to the processing of personal data for the provision of the service, the Customer is the Controller and Incision, in its capacity of Processor, processes the data on behalf of the Customer;
- Incision, in its capacity of Processor, for the provision of the Services will process only "common" personal data (name and surname, e-mail, role, structure) and other "common" personal data depending on the Services. Incision products are not meant to process special categories of personal data (art. 9, par. 1, GDPR).
- this DPA and its Annexes contain the terms and conditions under which Incision, in its capacity of Processor, shall process personal data on behalf of the Customer, in its capacity of Controller;
- the Controller agrees that Incision provides sufficient guarantees of expert and secured processing, implementing appropriate technical and organizational measures (see list of security measures in Annex 1) that meet the requirements of the Regulation EU 679/2016 (hereinafter "**GDPR**"); and
- this DPA is supplemental to and forms integral part of the Business Terms & Conditions. In case of any conflict, this DPA will take precedence over the terms of the Business Terms & Conditions.

The Parties agree as follows:

1. Duties of the Processor

The Processor shall:

a) Process personal data only for the purpose of performance of the Services, or as otherwise agreed within the lawful written instructions of the Controller.

b) Promptly inform the Controller in case the Processor becomes aware that one of Controller's instructions violate any relevant data protection legislation. In such case the Processor shall, where necessary, cease all processing. In the event this provision is invoked, the Processor shall not be liable for any failure to provide the Services.

c) Ensure that each of its employees that will need to access to personal data processed on behalf of the Customer:
   - received specific authorization, instructions, and training regarding the processing activity; and
   - has committed to confidentiality or is subjected to an appropriate obligation of confidentiality.

d) Ensure the respect of the security measures described in Annex 1. If the Controller requests the Processor in writing to implement or amend such security framework, the Processor will inform the Controller about the implementation and/or amendment costs; once the Controller has confirmed to bear such costs, the Processor will implement it without undue delay.

e) Assist the Controller, insofar as this is feasible and limited to the processing activities performed on behalf of the Customer:
   - For the fulfillment of the Controller's obligation to respond to requests of data subjects regarding the exercise of their rights; and
   - With all the information needed to perform a data protection impact assessment as required by art. 35 GDPR.

f) Make available to the Controller, upon its written request, information that demonstrates compliance with this DPA.

g) Notify to the Controller, without undue delay, in case a personal data breach occurred. In such event the Processor shall provide the following information:
   - A description of the incident and how it occurred;
   - Date and time of the incident and information about when/how the incident concluded (or the fact that the incident is still occurring);
   - The approximated amount and categories of personal data it involved;
   - The actual and likely consequences of the incident; and
   - The measures which have been or will be taken to resolve the Incident or to minimise its consequences.

h) Implement and keep up to date a register of processing activities as required by art. 30 GDPR.

i) Notify the Controller in advance if the Processor intends to outsource part or all processing activities, providing all necessary information to prove the security of the processing. The Controller has 30 days to oppose (in writing and for proved and well-founded reasons). The Processor shall impose the same requirements (or even stricter) to which it is subject itself under this DPA on the Sub-Processor. If a Sub-Processor fails to fulfill its data protection obligations, the Processor shall remain fully liable to the Controller for the performance of that Sub-Processor obligations. The Controller accept the Sub-Processors listed in Annex 2 and agrees that those Sub-Processors provide adequate guarantees regarding the security of the processing of personal data.

2. Duties and rights of the Controller

2.1 The Controller shall ensure the Processor that all personal data has been collected legitimately and that all data subjects have been informed of the processing of their personal data.

2.2 The Controller is entitled to conduct an audit on the processing of personal data by the Processor. In such case the Controller shall align with the Processor on a suitable date, time, duration, and manner and shall not unreasonably disturb the business of the Processor. Such audits can be performed by the Controller itself or by a third party hired by the Controller; in both cases the Controller shall bear all costs of the audit and share without undue delay the findings of the audit with the Processor.

2.3 For all relevant communications regarding the content of this DPA, the Controller shall use the following contact information: privacy.security@incision.care.

3. Liability

Reference is made to the Liability and Indemnification clauses of the Business Terms & Conditions.

4. Duration and termination

This DPA shall enter into force on the date of signing, and the duration of this DPA shall be the same one of the one of the contract(s) for the provision of the Services, terminating at the termination of the (last) contract for the provision of the Services, unless the processing of personal data continues, in which case the DPA shall remain in force.

5. Retention period

The retention periods are indicated in Annex 3.

6. Dispute Resolution and Governing Law

Reference is made to the Dispute Resolution and Governing Law clauses of the Business Terms & Conditions.

7. Final provisions

7.1 The recitals constitute integral part of this DPA.

7.2 In the event that one or more provisions of this DPA are rendered null or void, the other provisions shall remain in force completely.

ANNEX 1

Security measures

All Incision's products are protected by the following security measures.

Technical measures	
Measure	Description
Encryption at rest	All personal data in AWS databases are encrypted (AES-256)
Security in communications	Incision applies the protocol https to communicate with AWS databases
Backups	All personal data in AWS databases are regularly backed up in a separate environment. The backups are encrypted as well
Event logs	All events in AWS databases are logged. System admins audit these logs regularly
Automated alerts	Automated alerts are installed on AWS databases to notify in real time Incision and Levi9 about suspicious activities. The efficiency of the alarms has been tested
Firewall and antivirus	All Incision devices are protected by a firewall and an antivirus; both are updated regularly
AWS physical security	Physical barrier controls are used to prevent unauthorised entrance to AWS facilities; passage through the physical barriers requires either electronic access control validation or validation by security personnel. Employees and contractors are assigned photo-ID badges that must be worn. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn, and are continually escorted by authorised employees or contractors while visiting the facilities. All access points are maintained in a secured state and are monitored by video surveillance cameras designed to record all individuals accessing the facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorised access to the facilities, including monitoring points of vulnerability with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the facilities. All physical access to the facilities by employees and contractors is logged and routinely audited
Organizational measures	
Measure	Description
Redundant storing	All personal data in AWS are stored on multiple devices across a minimum of three Availability Zones (an Availability Zone is one or more discrete data centers with redundant power, networking, and connectivity in an AWS Region). These Services are designed to handle concurrent device failures by quickly detecting and repairing any lost redundancy, and they also regularly verify the integrity of the data using checksums
Employee access limitation	Incision employees access to AWS databases on a least privilege, access limitation, and need to know base
Employee training	All Incision employees received specific training regarding data protection and information security
Two factor authentication	All Incision employee that need to access AWS databases need to authenticate themselves through a 2FA process
Password manager	All Incision passwords are stored and protected by a professional password manager tool
Incident response plan and data breach notification policy	Incision adopted and shared with all its employees and (when appropriate) external partners an incident response plan and a data breach notification policy to be able to track, assess and report efficiently any incident occurred
Information security policy	Incision adopted and shared with all its employees an information security policy, to ensure and enhance the respect of its security practices
Privacy & Security organization	Incision set up an internal framework of roles and responsibilities regarding data protection and information security matters

ANNEX 2

Sub-Processors

The following providers are Sub-processors for the processing of personal data performed by Incision on behalf of the Customer. Incision imposed at least the same requirements to which it is subject itself under this DPA on all its providers.

Provider	Purpose	Storage location	Transfer out of EU?	Certifications
Amazon Web Services ("**AWS**")	Storage of all data processed by Incision's services	AWS Region (Ireland)	No	ISO/IEC 27001 ISO/IEC 27701
Levi9	Product maintenance	Levi9 only access, when needed, personal data without storing it	No	ISO/IEC 27001

ANNEX 3

Retention period

The retention period of personal data processed by Incision on behalf of the Customer depends on the product.

Incision Academy
At the termination of the contract with the Customer, Incision (after removing every reference of the Customer from its users' profiles) leaves the control of the personal data in the single account to the user (natural person). In fact, the single user could have the interest in keeping his/her account active or even choose to activate his/her own license to access Incision Academy content. Doing this, Incision becomes the Controller of that data (and fully accountable for compliance with all controller's data protection obligations) until the user decides to delete his/her account.
Incision Assist
At the termination of the contract with Incision, the Customer, with a written instruction, shall notify Incision to either delete or return all personal data processed on its behalf. In any case, Incision will promptly execute the request, notifying the Customer that Incision is no longer processing any personal data.