Data Processing Agreement

iCure Services and Cardinal

iCure SA (Switzerland) and iCure Belgium SRL (Belgium)

Version 2.0, effective 22 October 2026 for new Clients and, for Clients with an active subscription on that date, thirty (30) days after the notice sent to them. Replaces the Data Processing Agreement dated 30 June 2026.

How this DPA applies

This Data Processing Agreement (the "**DPA**") forms part of the iCure General Terms and Conditions (the "**GT&C**") and of every Sales Order concluded under them (together, the "**Agreement**"). It sets out the obligations of the parties under Article 28 of Regulation (EU) 2016/679 (the "**GDPR**") and Article 9 of the Swiss Federal Act on Data Protection of 25 September 2020 (the "**FADP**") when iCure processes Personal Data on behalf of the Client.

Acceptance. The Client accepts this DPA when it accepts the GT&C, by registering for, accessing or using the iCure Services (including any free subscription plan of Cardinal), or when it signs or accepts a Sales Order. No separate signature is required. A Client that needs a countersigned copy may request one at privacy@icure.com; the countersigned copy has the same content as the published version.

Contracting iCure entity. Each subscription covers one Hosting Region and is concluded with the iCure entity of that region, which is also the entity named in the Sales Order. "**iCure**" means that entity:

- **EU Hosting Region:** iCure Belgium SRL, Avenue des Eaux Vives 4, 1332 Genval, Belgium, company number BE 1017.767.847;
- **Swiss Hosting Region:** iCure SA, Route de la Corniche 2, 1066 Epalinges, Switzerland, IDE CHE-270.492.477.

Each iCure entity is solely responsible for the processing it performs under its own subscriptions and Sales Orders. A Client hosted in both Hosting Regions has a separate contractual relationship with each entity. The Client and iCure are each a "**party**".

Negotiated DPA. Where the Client and iCure have signed a data processing agreement that expressly replaces this DPA, the signed agreement prevails.

Language. This DPA is drafted in English. Any translation is provided for convenience only; the English version prevails.

1 Definitions

1.1 Capitalised terms not defined in this DPA have the meaning given to them in the GT&C. The terms "controller", "processor", "Data Subject", "processing", "Personal Data", "Personal Data Breach" and "Supervisory Authority" have the meaning given to them in the Applicable Data Protection Law; where the FADP applies, they include the corresponding FADP notions, in particular "breach of data security" and the Federal Data Protection and Information Commissioner.

1.2 In this DPA:

"Account Data" means Personal Data of the Client's Account Owners, billing contacts and other representatives that iCure processes to manage the Client's account, billing, security and support.

"Account Owner" means a person, typically a developer or administrator of the Client, who has created or manages an account of the Client in the Cardinal Cockpit or any other iCure interface.

"Applicable Data Protection Law" means the GDPR, the Belgian Law of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, the FADP and the Swiss Data Protection

Ordinance of 31 August 2022 (the "**FDPO**"), and any other data protection law applicable to the processing under this DPA.

"Client Personal Data" means the Personal Data contained in Client Data, or otherwise processed by iCure on behalf of the Client under the Agreement, as described in Annex 3.

"Encrypted Data" means Client Data encrypted end-to-end with the encryption features of the iCure Services, so that it can only be decrypted with the corresponding Encryption Keys.

"Encryption Keys" means the private keys needed to decrypt Encrypted Data, held by the Client, its End Users or devices under their control.

"End User" means any person who uses an application or service of the Client built on the iCure Services, including healthcare professionals, members of care teams and patients.

"Hosting Region" means the region, EU or Switzerland, in which the Client's databases are hosted, as selected by the Client when subscribing or as stated in the Sales Order.

"Sub-processor" means any processor engaged by iCure, or by another Sub-processor, that processes Client Personal Data or has access to systems storing it, including infrastructure providers that only have physical access to those systems.

2 Roles and scope

2.1 **iCure as processor.** For Client Personal Data, the Client acts as controller and iCure acts as processor.

2.2 **Client acting as processor.** Where the Client processes Client Personal Data on behalf of one or more third-party controllers (for example as a software vendor serving hospitals, practices or healthcare professionals), iCure acts as a sub-processor of the Client. In that case the Client:

(a) warrants that its instructions to iCure, including the engagement of iCure and of the Sub-processors listed in Annex 1, are authorised by those controllers;

(b) remains iCure's sole point of contact and relays any communication between iCure and those controllers; and

(c) is not required to disclose the identity of those controllers to iCure, but discloses it to iCure or to a Supervisory Authority where the law requires it.

References in this DPA to the Client as controller then apply to the Client acting on the instructions of those controllers.

2.3 **Account Data.** iCure processes Account Data as a controller, in accordance with its Privacy Policy published at https://cardinalsdk.com/en/legal/. This DPA does not apply to Account Data.

2.4 **Services covered.** This DPA applies to all iCure Services, whatever the subscription plan, and to any support, maintenance or professional services in the course of which iCure processes Client Personal Data.

2.5 **Compliance.** Each party complies with the Applicable Data Protection Law. The Client is responsible for the lawfulness of the processing it instructs, including the legal basis and, for health data, the applicable condition under Article 9 GDPR or the FADP, for informing Data Subjects, and for the accuracy of Client Personal Data. The Client informs iCure without undue delay at privacy@icure.com if it becomes aware that the processing under this DPA does not comply with the Applicable Data Protection Law.

2.6 **Details of the processing.** The subject matter, duration, nature and purpose of the processing, the categories of Personal Data and the categories of Data Subjects are described in Annex 3.

3 Instructions

3.1 iCure processes Client Personal Data only on documented instructions from the Client, including with regard to transfers outside the Hosting Region. The Agreement, this DPA, and the Client's configuration and use of the iCure Services (including the API calls made by its applications) are the Client's complete instructions at

the date of acceptance. Further instructions must be given in writing; where they require work outside the standard iCure Services, they may be subject to a Sales Order.

3.2 iCure may process Client Personal Data otherwise only where required to do so by the law of the European Union, of an EU Member State or of Switzerland to which iCure is subject. In that case iCure informs the Client of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.3 iCure informs the Client without delay if, in its opinion, an instruction infringes the Applicable Data Protection Law, with a reasonably detailed explanation. iCure may suspend the execution of that instruction until the Client confirms or modifies it.

3.4 iCure does not process Client Personal Data for its own purposes, does not sell it and does not use it for commercial or marketing purposes. This does not prevent iCure from using technical telemetry on the use and performance of the iCure Services (such as request volumes, error rates and storage usage), which does not include the content of Client Data and does not identify Data Subjects, to operate, secure and improve the iCure Services.

4 End-to-end encryption

4.1 The iCure Services provide end-to-end encryption. The Client decides, through its configuration and use of the iCure Services, which Client Data is encrypted end-to-end.

4.2 Encryption Keys are generated and kept on the side of the Client and its End Users. The iCure Services are designed so that neither iCure nor its Sub-processors hold Encryption Keys or can decrypt Encrypted Data. iCure accesses decrypted Client Data only if the Client gives it explicit written authorisation and the means to do so; such access is then an instruction under Section 3.

4.3 Client Data that is not encrypted end-to-end, such as identification data needed to authenticate users, technical metadata needed to operate the iCure Services and fields that the Client chooses to leave unencrypted, is protected by encryption in transit and at rest and by the other measures described in Annex 2.

4.4 The Client is responsible for the custody of Encryption Keys and for using the key recovery mechanisms offered by the iCure Services. iCure cannot restore Encrypted Data whose Encryption Keys have been lost.

4.5 Client Personal Data is protected under this DPA whether or not it is encrypted. Encryption is a security measure; it does not reduce the obligations of either party under this DPA.

5 Confidentiality and professional secrecy

5.1 iCure ensures that every person acting under its authority who may access Client Personal Data (a) is bound by a written confidentiality undertaking or by an appropriate statutory obligation of confidentiality, (b) has been informed of the sanctions applicable to a breach of confidentiality, and (c) processes Client Personal Data only on iCure's instructions, unless required otherwise by law.

5.2 Where Client Personal Data is covered by a professional secrecy obligation of the Client or of the controllers on whose behalf it acts, in particular medical secrecy under Article 321 of the Swiss Criminal Code or the corresponding rules of Belgian or other applicable law, iCure:

(a) keeps that data secret and does not seek to obtain knowledge of it;

(b) invokes, to the extent available to it, the rights of auxiliaries of persons bound by professional secrecy to refuse to testify and to oppose the seizure of documents (in Switzerland, Articles 171 and 264 of the Swiss Criminal Procedure Code); and

(c) binds its Sub-processors to confidentiality obligations appropriate to that secrecy.

6 Security of processing

6.1 iCure implements and maintains technical and organisational measures ensuring a level of security appropriate to the risk, as required by Article 32 GDPR and by Article 8 FADP together with Articles 1 to 5 FDPO, in particular against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Client Personal Data. These measures are described in Annex 2.

6.2 iCure operates an information security management system certified to ISO/IEC 27001 and holds the other certifications listed in Annex 2. iCure informs the Client without undue delay if a certification listed in Annex 2 is suspended or withdrawn.

6.3 iCure may update the measures described in Annex 2 to follow technical and regulatory developments, provided that the overall level of protection of Client Personal Data is not reduced.

7 Sub-processors

7.1 **General authorisation.** The Client gives iCure a general written authorisation to engage Sub-processors, within the meaning of Article 28(2) GDPR and Article 9(3) FADP with Article 7 FDPO. The Sub-processors engaged at the effective date of this DPA are listed in Annex 1, by Hosting Region; the current list is also published at https://cardinalsdk.com/en/legal/. Only the Sub-processors listed for the Client's Hosting Region, and those listed as common to all Hosting Regions, process the Client's Personal Data.

7.2 **Flow-down.** iCure engages a Sub-processor only under a written contract imposing the data protection obligations required by Article 28(4) GDPR and Article 9 FADP, with sufficient guarantees as regards security measures, confidentiality, notification of Personal Data Breaches and audits. Where iCure negotiates the contract, these obligations are at least as protective as those of this DPA. A Sub-processor engaged by another Sub-processor requires iCure's prior authorisation and is listed in Annex 1; for infrastructure providers contracting on standard terms, Annex 1 refers to the lists of sub-processors they publish.

7.3 **Responsibility.** iCure remains fully responsible towards the Client for the performance by its Sub-processors of their data protection obligations.

7.4 **Changes.** iCure informs the Client of any intended addition or replacement of a Sub-processor at least thirty (30) days before the change, by email to the Account Owner and by updating the published list. Where the change concerns a Sub-processor engaged by another Sub-processor and iCure is informed of it with shorter notice, iCure informs the Client as soon as it is itself informed. Where an emergency affecting the security or continuity of the iCure Services requires it, iCure may replace a Sub-processor immediately, within the same Hosting Region and with equivalent safeguards, and informs the Client without undue delay afterwards.

7.5 **Objection.** The Client may object to a change on reasonable data protection grounds by writing to privacy@icure.com within thirty (30) days of the notice. The parties then seek a solution in good faith. If no solution is found within thirty (30) days of the objection, the Client may terminate the affected iCure Services without penalty by written notice, and iCure refunds any prepaid fees for the period after termination. Where the notice is given after the change under Section 7.4, the objection period runs from that notice. In the absence of objection within the notice period, the change is deemed accepted.

8 Location of processing and international transfers

8.1 **Hosting Region.** iCure stores Client Personal Data in the Hosting Region selected by the Client:

(a) for the EU Hosting Region, in the European Union;

(b) for the Swiss Hosting Region, in Switzerland, including replicated copies of the databases.

iCure does not move Client Personal Data to another Hosting Region without the Client's instruction. A change of Hosting Region requires a new Sales Order with the iCure entity of the new Hosting Region.

8.2 **Transfers.** Any transfer of Client Personal Data outside the Hosting Region, including remote access from another country by personnel of iCure or of a Sub-processor, takes place only (a) to a country recognised as

providing an adequate level of data protection under Article 45 GDPR or Article 16(1) FADP, or (b) under appropriate safeguards, such as the standard contractual clauses adopted by the European Commission, with the adaptations required by the FADP where Swiss law applies. The European Union recognises Switzerland, and Switzerland recognises the Member States of the European Union, as providing an adequate level of protection. Annex 4 describes the safeguards relied upon.

8.3 **French health data.** Where the Client stores health data covered by Article L.1111-8 of the French Public Health Code, the Client must select the EU Hosting Region; the Swiss Hosting Region is outside the scope of iCure's HDS certification. The information on transfers, remote access and exposure to non-European laws that certified health data hosts must publish is set out in Annex 4 and kept up to date.

9 Assistance to the Client

9.1 **Data Subject requests.** The iCure Services provide technical means, through their APIs and features, to access, rectify, export, restrict and erase Client Personal Data, including Encrypted Data in its encrypted form. If iCure receives a request from a Data Subject relating to Client Personal Data, it forwards the request to the Client without undue delay and does not respond to it unless the Client authorises it to do so. As iCure cannot decrypt Encrypted Data, its assistance in respect of Encrypted Data is limited to those technical means. Erased data remains in backup copies until they expire under the backup cycle described in Annex 2.

9.2 **Other obligations.** Taking into account the nature of the processing and the information available to it, iCure assists the Client in ensuring compliance with Articles 32 to 36 GDPR and Articles 8 and 22 to 24 FADP, in particular by providing information on its security measures, its certifications and its Sub-processors (including their own certifications) for data protection impact assessments and prior consultations of Supervisory Authorities.

9.3 **Costs.** Assistance going beyond the documentation and self-service features of the iCure Services may be charged at iCure's standard rates, unless it is needed because of a breach of this DPA by iCure.

10 Personal Data Breach

10.1 iCure notifies the Client without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Client Personal Data, including a Personal Data Breach occurring at a Sub-processor.

10.2 The notification is sent to the Account Owner and to the privacy contact designated by the Client in the Cardinal Cockpit. The Client keeps these contact details up to date.

10.3 The notification describes, as far as the information is available, the nature of the Personal Data Breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed, and a contact point. Information not available at first is provided in phases without undue delay. iCure states whether the data concerned was Encrypted Data and whether Encryption Keys may have been compromised, so that the Client can assess its own notification obligations.

10.4 iCure takes reasonable measures to contain the Personal Data Breach, mitigate its possible adverse effects and prevent recurrence, and cooperates with the Client in its investigation. iCure documents every Personal Data Breach, including the facts, its effects and the remedial action taken, and provides that documentation to the Client on request. A notification is not an acknowledgement of fault or liability.

10.5 The Client remains responsible for notifying Supervisory Authorities and Data Subjects where required. iCure does not notify them on the Client's behalf unless the Client instructs it to do so or the law requires it.

11 Records and audits

11.1 **Records.** iCure keeps a record of the processing activities it carries out on behalf of its clients, as required by Article 30(2) GDPR and Article 12 FADP, and makes the relevant information available to the Client on request.

11.2 **Documentation.** iCure makes available to the Client the information necessary to demonstrate compliance with this DPA, in particular its certificates, a summary of its most recent external audit and penetration test, Annex 2 and, for Sub-processors, their certifications and, where the Sub-processor permits it, their audit reports or summaries of them (for example the Tier IV certification and ISAE 3402 Type 2 report of the Swiss Hosting Region datacenter). This information is Confidential Information of iCure.

11.3 **On-site audits.** Where the information under Section 11.2 is not sufficient to demonstrate compliance, where a Supervisory Authority requires it, or after a Personal Data Breach, the Client may audit iCure, itself or through an independent auditor bound by confidentiality who is not a competitor of iCure. The Client sends its request, with a proposed scope, at least twenty (20) working days in advance to privacy@icure.com. Audits take place during business hours, without disrupting the iCure Services, at most once per calendar year except after a Personal Data Breach or at the request of a Supervisory Authority, and are limited to the processing of Client Personal Data. The Client keeps all information obtained during the audit confidential and shares the audit report with iCure.

11.4 **Sub-processors.** Sub-processors are audited by iCure under its contracts with them or through their certifications and audit reports. Where the information under Section 11.2 is not sufficient, the Client may request an audit of a Sub-processor with the same notice; iCure organises it to the extent its contract with the Sub-processor allows, at the Client's cost, with an auditor who is not a competitor of iCure or of the Sub-processor.

11.5 **Costs.** Each party bears its own audit costs. iCure's time beyond one working day per audit is charged at CHF 1,000 (iCure SA) or EUR 1,000 (iCure Belgium SRL) per day or part of a day, unless the audit reveals a material breach of this DPA by iCure.

12 Requests from authorities and third-party measures

12.1 If iCure receives a request or order from an authority or any other third party to disclose Client Personal Data, iCure (a) redirects the requester to the Client where possible, (b) informs the Client without delay unless legally prohibited from doing so, and (c) discloses only what it is legally required to disclose, after assessing the lawfulness of the request and using the available remedies where reasonable. As iCure does not hold Encryption Keys, it can only disclose Encrypted Data in encrypted form.

12.2 If Client Personal Data held by iCure or by a Sub-processor is endangered by a seizure, an attachment, insolvency or composition proceedings or any other third-party measure, iCure informs the Client without delay and informs the authorities and persons concerned that the Client, or the controllers on whose behalf it acts, alone control that data.

13 Return and deletion of data

13.1 During the Agreement, the Client can export Client Data at any time through the APIs of the iCure Services.

13.2 On termination or expiry of the Agreement for any reason, iCure stops processing Client Personal Data other than as provided in this Section 13, and:

(a) keeps Client Data for sixty (60) days after the end of the iCure Services (the "**Retrieval Period**"), during which the Client may request its return by email to privacy@icure.com;

(b) on such request, returns Client Data in a structured, commonly used, machine-readable and interoperable format within twenty (20) working days, and keeps it until the return is completed; Encrypted Data is returned in encrypted form;

(c) at the end of the Retrieval Period, or earlier on the Client's written request, deletes Client Personal Data and all copies. Copies held in backups are deleted at the end of the backup cycle described in Annex 2, and in any event within twelve (12) months, and remain protected under this DPA until then.

13.3 iCure may keep Client Personal Data where the law of the European Union, of an EU Member State or of Switzerland requires it, only for the purpose and duration required and subject to this DPA.

13.4 On request, iCure confirms the deletion in writing.

13.5 For free subscription plans, iCure deletes the Client's entire database, including all Client Data, after twelve (12) months without activity. Activity means any authenticated access to that database through the iCure Services or their APIs. iCure informs the Account Owner by email at least one (1) month before deletion, so that the Client can export its data under Section 13.1; backup copies follow Section 13.2(c). For trial periods, the GT&C apply.

14 Liability

14.1 Each party is liable for damage caused by the processing attributable to it, in accordance with the Applicable Data Protection Law. iCure is liable for damage caused by the processing only where it has not complied with the obligations of the Applicable Data Protection Law specifically directed to processors or with this DPA, or where it has acted outside or contrary to lawful instructions of the Client.

14.2 The aggregate liability of each party arising out of or in connection with this DPA and the Applicable Data Protection Law, including in respect of Personal Data Breaches, is limited to the greater of (a) three (3) times the fees paid or payable by the Client for the hosting and processing of Client Data by the affected iCure Services in the twelve (12) months preceding the first event giving rise to liability, as identified in the Sales Order or the applicable price list, excluding fees for support packages, maintenance and support agreements, professional services, non-recurring engineering (NRE) and other additional services, and (b) CHF 1,000 (iCure SA) or EUR 1,000 (iCure Belgium SRL). For such claims, this cap replaces the general cap of the Agreement, and amounts paid under it do not count towards the general cap. The other limitations and exclusions of liability of the Agreement (Section 15 of the GT&C) continue to apply; however, the reasonable costs of investigating a Personal Data Breach caused by a breach of this DPA by iCure, and of notifying it to Supervisory Authorities and Data Subjects, are direct damages recoverable within this cap. Nothing in this DPA limits liability that cannot be limited under applicable law.

14.3 Where a party has paid full compensation to a Data Subject for damage for which the other party is responsible in whole or in part, it may claim back from the other party the part of the compensation corresponding to that party's responsibility.

15 Term, precedence and amendments

15.1 **Term.** This DPA applies for as long as iCure processes Client Personal Data, including during the Retrieval Period and until deletion.

15.2 **Precedence.** In case of conflict on data protection matters, this DPA prevails over the GT&C and any Sales Order, unless a Sales Order signed by both parties expressly derogates from a specific Section of this DPA. Standard contractual clauses entered into under Section 8.2 prevail over this DPA.

15.3 **Amendments.** iCure may amend this DPA to reflect changes in the Applicable Data Protection Law, in the iCure Services or in its Sub-processors (Section 7 then applies). iCure informs the Client of material amendments by email at least thirty (30) days before they take effect. No amendment may reduce the overall level of protection of Client Personal Data during a committed subscription term. A Client that objects may terminate the affected iCure Services without penalty before the amendment takes effect; continued use after that date is acceptance. Each published version is dated, and earlier versions are available on request.

15.4 **Notices.** Notices to iCure under this DPA are sent to privacy@icure.com. Notices to the Client are sent to the email address of the Account Owner.

15.5 **Severability.** If a provision of this DPA is or becomes invalid, it is replaced by a valid provision whose effect is as close as possible to the invalid one; the other provisions remain in force.

16 Governing law and jurisdiction

16.1 This DPA is governed by the law that governs the GT&C for the contracting iCure entity: Swiss law where iCure SA is the contracting entity, and Belgian law where iCure Belgium SRL is the contracting entity.

16.2 The parties first attempt to settle any dispute amicably. Failing that, the courts of Lausanne have exclusive jurisdiction where iCure SA is the contracting entity, and the French-speaking courts of Brussels have exclusive jurisdiction where iCure Belgium SRL is the contracting entity.

16.3 This Section does not affect the rights of Data Subjects or the competence of Supervisory Authorities under the Applicable Data Protection Law.

Annex 1: Sub-processors

Sub-processors are listed by Hosting Region. A Client only has its Personal Data processed by the Sub-processors of its own Hosting Region and by those listed under A. Infrastructure providers contracting on standard terms (OVHcloud, Google Cloud) use their own sub-processors, listed on their published sub-processor pages. The current list is also published at https://cardinalsdk.com/en/legal/.

A. All Hosting Regions

Sub-processor	Purpose	Access to Client Personal Data	Location
iCure SA or iCure Belgium SRL, whichever is not the contracting entity	Intra-group operation, administration and support of the platform	Administrative access to production systems; no access to Encryption Keys	Switzerland / Belgium

B. EU Hosting Region (contracting entity: iCure Belgium SRL)

Sub-processor	Purpose	Access to Client Personal Data	Location
OVH SAS (OVHcloud), 2 rue Kellermann, 59100 Roubaix, France (RCS Lille Métropole 424 761 419)	Hosting and infrastructure	Data hosting on mirrored servers	Strasbourg (France) and Limburg (Germany), EU
Google Cloud EMEA Limited (Ireland), Google Cloud Platform; contracted through the reseller Devoteam G Cloud BeLux, Diegem, which has no access to Client Personal Data	Application servers (computing)	Transient processing of requests; no storage of Client Data; no Encryption Keys	Belgium (EU); safeguards in Annex 4
Passmann Benelux (formerly Taktik), Avenue Reine Astrid 92, 1310 La Hulpe, Belgium	Backup storage	Storage of encrypted backups	Belgium (EU)

C. Swiss Hosting Region (contracting entity: iCure SA)

Sub-processor	Purpose	Access to Client Personal Data	Location
Edificom SA, Route de la Corniche 1, 1066 Epalinges (CHE-111.720.820)	Provision and maintenance of physical servers and network connectivity	Physical access to servers only; no logical access; no access to Encryption Keys	Switzerland
BrainServe SA, Rue de la Vernie 12, 1023 Crissier (sub-processor of Edificom SA)	Datacenter colocation: physical hosting of servers and network connectivity	Physical access to the datacenter only; no logical access; no access to Encryption Keys	Crissier (VD), Switzerland
synaforce Schweiz AG (formerly ServerBase AG), Bachenbülach (ZH) (CHE-115.419.029)	Database storage and replication	Encrypted replication, on two separate physical sites	Winterthur (ZH) and Lupfig (AG), Switzerland

Edificom SA is contractually responsible towards iCure SA for the compliance of BrainServe SA with the physical security obligations of their data processing agreement. The BrainServe datacenter is certified Tier IV by the Uptime Institute and audited annually under ISAE 3402 Type 2 and FINMA Circular 2018/3.

Annex 2: Technical and organisational measures

This Annex describes the main measures iCure implements to protect the iCure Services and the data stored through them against malicious or accidental unauthorised access, loss or alteration. iCure reviews and improves these measures continuously.

A2.1 Certifications and governance

- **ISO/IEC 27001:2022.** iCure SA and iCure Belgium SRL operate a certified information security management system, audited by TÜV AUSTRIA Hellas. Internal audits and staff training take place between external audits.
- **HDS.** Certification as a French health data host (hébergeur de données de santé), activities 3 to 5, for the EU Hosting Region, issued by CertiTrust.
- **ISO 13485:2016.** Certified quality management system for the design and development of the iCure Services.
- **Test data.** No production data is used in test environments.
- **Zero trust.** A single security standard applies to every connected device, whether used by iCure personnel and contractors or by Clients accessing their own data.

A2.2 Encryption and access control

- **End-to-end encryption.** The iCure Services offer asymmetric end-to-end encryption by default. Users select the data to encrypt within a database, so that sensitive data stays encrypted while the unencrypted part can still be processed automatically.
- **Design objectives of the encryption model:** each data owner has a public and private key pair; a data owner can decrypt the data it created or that was shared with it, starting from its private key only; a data owner cannot decrypt data that was not shared with it; third parties cannot access sensitive data, nor infer relationships between entities that would reveal sensitive information (for example the frequency of a patient's visits); a data owner who loses its private key can regain access to data it had shared with other data owners.
- **No access by iCure.** The iCure Services are designed so that iCure does not hold Encryption Keys. Unless the Client provides the means under Section 4.2, Encrypted Data is not available in decrypted form to iCure personnel or to any Sub-processor.
- **Data not encrypted end-to-end** is encrypted in transit (TLS) and at rest, in both Hosting Regions.
- **Granular permissions.** The data model applies a cascade of permissions to every item of data within a Client database, so that each user only accesses the data appropriate to its role.
- **Administrative access** to production systems is limited to authorised personnel and protected by multi-factor authentication.
- **Logging and processing regulation.** End-to-end encryption is the primary preventive measure. In addition, access to and changes of personal data are logged in accordance with Article 4 FDPO, and iCure's ISO/IEC 27001 documentation, which covers iCure SA and iCure Belgium SRL, serves as the processing regulation required by Article 5 FDPO.

A2.3 Infrastructure of the EU Hosting Region

- **OVHcloud.** Data is stored on mirrored servers in the OVHcloud datacenters of Strasbourg (France) and Limburg (Germany); backups are kept separately by Passmann Benelux in Belgium.
- **Google Cloud Platform** (Google Cloud EMEA Limited), contracted through Devoteam G Cloud BeLux, runs the application servers in Belgium. No Client Data is stored and no Encryption Keys are kept on Google Cloud.
- **Passmann Benelux** (formerly Taktik). Backup storage in Belgium.
- OVHcloud and Google Cloud are certified ISO/IEC 27001 and HDS; Passmann Benelux is certified ISO 9001 and ISO/IEC 27001.

A2.4 Infrastructure of the Swiss Hosting Region

iCure SA runs the Swiss Hosting Region on physical servers provided and maintained by Edificom SA in the BrainServe SA datacenter in Crissier (VD). Edificom SA has physical access to the servers only; it has no logical access to operating systems, databases or data and never holds Encryption Keys. All data stored on these servers is encrypted, end-to-end or at rest, with keys that are not accessible to Edificom SA. The databases of the Swiss Hosting Region are stored and replicated, encrypted, by synaforce Schweiz AG (formerly ServerBase AG) on two separate physical sites in Winterthur (ZH) and Lupfig (AG). The measures of Edificom SA and BrainServe SA include:

- **Datacenter:** Tier IV certification by the Uptime Institute; annual ISAE 3402 Type 2 audit; compliance with FINMA Circular 2018/3; operations based on ISO 20000 and ITIL; on-site monitoring 24 hours a day, 365 days a year; location outside identified natural and industrial risk zones; proprietary fibre network around Lausanne connected to the main interconnection points.
- **Physical access:** strict access control to premises and server rooms, limited to expressly authorised persons; CCTV and access logs; identification and authentication of technicians; mandatory escort of third parties in sensitive areas; locked rooms and racks; register of physical access available to iCure SA.
- **Continuity:** redundant power supply (dual feed, UPS, generators) and cooling; documented backup and restoration of hardware configurations; business continuity and disaster recovery plan; physical intrusion tests at least once a year.
- Personnel of Edificom SA and BrainServe SA are bound by confidentiality and professional secrecy obligations equivalent to Section 5 of this DPA.

A2.5 Availability and resilience

- Service levels are set out in Annex I of the GT&C or, where applicable, in the Client's Maintenance and Support Agreement.
- Data is stored on mirrored servers, with an extensive backup policy in the hosting infrastructure. Data reconciliation and conflict resolution are built into the iCure Services.
- **Backup cycle:** a daily backup kept for one week, a weekly backup kept for one month, a monthly backup kept for three months and a quarterly backup kept for one year. Backups are not modified after creation; they expire at the end of this cycle.
- Restoration from backup is tested at least once a year, with documented results.

A2.6 Supplier management

- All suppliers are vetted before engagement and bound by a security policy proportionate to their access. Sub-processors are bound by the obligations described in Section 7, and their certifications are monitored.

Annex 3: Description of the processing

A3.1 Subject matter, nature and purposes

iCure processes Client Personal Data to provide, operate, secure and support the iCure Services subscribed by the Client, as further instructed by the Client through its use of the iCure Services. The processing consists of:

- hosting, storage, backup and restoration of Client Data;
- support for the encryption of Client Data, and synchronisation and transmission of Client Data between the Client's applications and End Users;
- technical operations needed to run and secure the iCure Services, including monitoring, maintenance and support;
- disclosure where required by law, under Section 12.

A3.2 Duration

The term of the Agreement, followed by the Retrieval Period and deletion under Section 13.

A3.3 Categories of Data Subjects

- End Users of the Client's applications: healthcare professionals, members of care teams, patients and their representatives;
- staff and users of the Client and of the controllers on whose behalf it acts;
- Account Owners and administrators of the Client's databases, insofar as their data is part of Client Data.

A3.4 Categories of Personal Data

- identification and contact data: name, email address, telephone number, postal address;
- national identification numbers, where the Client is authorised by law to process them (for example the Belgian national register number, NISS; in Switzerland, the AHV number only where its systematic use is authorised by law);
- authentication and technical data: user identifiers, credentials in protected form, IP addresses, device identifiers, logs and timestamps;
- any other data the Client or its End Users enter or upload, which may be Encrypted Data.

A3.5 Special categories of data

Health data and other special categories of Personal Data within Article 9 GDPR, and sensitive personal data within Article 5(c) FADP, as determined by the Client. The Client is expected to encrypt such data end-to-end. Because iCure cannot see Encrypted Data, it relies on the Client to determine the categories of data processed; the Client informs iCure if it processes data requiring specific measures, such as genetic data or data of minors on a large scale.

A3.6 Frequency and Sub-processors

Continuous processing for the duration of the iCure Services. Sub-processors are listed in Annex 1.

Annex 4: Transfers and exposure to non-European laws

A4.1 Transfer safeguards

- **Between the European Union and Switzerland:** adequacy decisions of the European Commission for Switzerland and of the Swiss Federal Council for the Member States of the European Union (Annex 1 FDPO).
- **Google Cloud Platform:** Google Cloud EMEA Limited (Ireland) runs the application servers in the EU and stores no Client Data. EU standard contractual clauses, Module 3 (processor to processor), incorporated in Google Cloud's terms and available at https://cloud.google.com/terms/sccs/eu-p2p, apply to any transfer outside the European Union by Google group entities.

- **Remote administration:** the platform is administered from Belgium. Administration of the Swiss Hosting Region from Belgium relies on the recognition of the EU Member States by the Swiss Federal Council. The EU Hosting Region is not administered from outside the European Union.
- **Swiss Hosting Region database replication:** stored in Switzerland (Winterthur and Lupfig); no transfer abroad.

A4.2 Information required from certified health data hosts (EU Hosting Region)

This section sets out, for the EU Hosting Region covered by iCure's HDS certification, the information on transfers, remote access and exposure to non-European laws that French law requires certified health data hosts to publish.

- **Storage:** health data subject to HDS certification is stored exclusively in the European Union, by OVHcloud in Strasbourg (France) and Limburg (Germany). Google Cloud Platform runs the application servers in Belgium and stores no data. iCure does not provide externalised backup (activity 6); the backups kept by Passmann Benelux in Belgium, which is not HDS certified, contain no health data subject to HDS certification.
- **Remote access from outside the European Union:** none. The EU Hosting Region is administered from the European Union only.
- **Exposure to non-European laws:** Google Cloud EMEA Limited belongs to a group whose parent company, Google LLC, is established in the United States. United States laws, such as the CLOUD Act and Section 702 of the Foreign Intelligence Surveillance Act, may allow United States authorities to request data from the group. OVH SAS and Passmann Benelux (Passmann group, France) are European companies.
- **Residual risk and measures:** no Client Data and no Encryption Keys are stored on Google Cloud. Encrypted Data stays encrypted on the application servers, since it is decrypted only on the side of the Client and its End Users. Data not encrypted end-to-end is processed there only transiently, in memory, while requests are handled, and travels encrypted (TLS). Requests received by iCure itself are handled under Section 12.

End of the Data Processing Agreement.