VideoLab GDPR Compliance Checklist

This document briefly summarizes the essential GDPR topics and how we have tackled them in collaboration with a typical controller.
Note that VideoLab processes two categories of data, namely non-sensitive user information and sensitive patient data. This document only describes the latter.

Controller and processor

The institution that deploys VideoLab for the educational purposes has the role of the **controller**. Codific has the role of the **processor**.

Lawfulness, fairness and transparency

Patient consult recordings are lawful in all EU countries given a freely given patient consent and the appropriate security measures in place.

Purpose limitation

Purposes of the processing are defined by the controller. Typically recordings are processed for the purposes of assessment and/or training of physicians in training.

Data minimisation

Identifiable patient data is only contained within audio / video recordings. Hence, data is minimized by definition.

Storage limitation and data hosting

All data is automatically destroyed after a fixed period of time defined by a system-wide parameter. Typically this setting is defined by the training period (e.g., 12 months). There is a single encrypted backup of the recording which is destroyed as well.
All data is stored within the EU. All data is encrypted using a state-of-the-art encryption and an advanced encryption key management system. A “two-man rule” is enforced for any master-key access to the system, which means that rare glass-break procedures can be applied when necessary.

Integrity and confidentiality (Security)

Please consult the “Security and Privacy Assessment” document for more information on security.

Lawful basis for processing: Consent

Patient data processing is consent-based. It is the obligation of the physician in training who makes the recording to ask for consent before the actual recording is started. If the patient agrees the consent must be asked and given once again on the recording. VideoLab only

processes video/audio recordings that contain identifiable information on the patient. No metadata is processed.

Patient rights

Data subject rights are very limited within VideoLab as we only process patients' recordings. Patients may exercise their right to object and rights to erasure by asking their physician in training who made the recording to simply delete it. Nobody else can delete the recordings. Glass break procedures are enforced by a two-man rule in case the physician in training who made the recording is unavailable.
Other data subject rights (rights to rectification, rights to data portability, rights to restrict processing, rights related to automated decision making and profiling, rights to be informed) are clearly out of scope.

Contracts

A controller / processor agreement is set up before the actual deployment of VideoLab where GDPR specifics are further detailed.

Privacy by design and by default

VideoLab is developed by leveraging LINDDUN - the most renowned methodology for privacy by design and by default.

Data protection impact assessment

Please consult the "Security and Privacy Assessment" document, which is the technical DPIA.

Data protection officer

Codific collaborates closely with the data protection officer (DPO) appointed by the controller.

Certification

Codific is ISO27001 certified. Please consult the "Declaration of applicability" document for further information regarding the implemented controls and responsibilities.