EKARE

GDPR Whitepaper

eKare Europe inSight

This white paper answers questions about the use of eKare inSight in view of the General Data Protection Regulation, the EU's latest privacy legislation which came into force on 25 May 2018. It will look at how eKare inSight complies with the requirements of the GDPR in terms of privacy protection and data security.

This white paper was published on 7 October 2020 by eKare Europe and is reviewed annually.

This white paper was compiled on the basis of interviews with stakeholders. The managers of those stakeholders have declared in writing that the content of this white paper provides an accurate picture of the current situation

Index

1. GDPR and Healthcare

The General Data Protection Regulation (GDPR) has had a huge impact on the healthcare sector. Medical data is now legally classed under special categories of personal data. These special categories of personal data fall under the ‘increased risk’ class, meaning that processing such data unlawfully can hugely affect the person to whom the data relates, i.e. the Data Subject.

For that reason and others, healthcare facilities must adopt technical and organizational measures to guarantee the confidentiality, integrity, and availability of personal data. These aspects also form an integral part of data security. Organizations that have already implemented a detailed data security policy (on the basis of the Dutch NEN 7510 standard, for example) are at an advantage.

In addition to the traditional aspects of data security, the GDPR also requires a number of specific processes and measures to be put in place to protect privacy. This includes listing which categories of personal data are processed by the organization, the purposes for which such data is processed, and what the lawful basis for the processing is. Each item of personal data should also be allocated a retention period, after which time the organization has to ensure that the personal data in question is destroyed or anonymized. These items should also be included in the ‘processing record’.

In addition to setting up processes to comply with the retention period, it is also important to take data minimization into account when compiling the policy. Simply put, this means that you as an organization must ensure that no more data is collected than necessary in order to deliver your product or service, and as little data is stored as possible.

Many organizations have already incorporated a number of requirements from the GDPR into their services organically. This includes informing data subjects of any data breaches so as to mitigate any potential adverse effects and allowing them to exercise their rights with ease. These processes often merely need to be strengthened in view of the GDPR.

By doing all of the above, this can help to underscore the principle of transparency, so you know how we process your data and how we guarantee your privacy on the basis of the requirements of the GDPR. We do this by publishing notifications (privacy statements) and consent procedures.

The requirements under the GDPR should be implemented within the organization both technically and organizationally. This means that all resources and systems should be designed to meet the requirements of the GDPR (technical) and that employees must fully comply with these requirements (organizational) when processing personal data.

The following sections of this white paper explain how eKare inSight serves as a technical measure to ensure privacy is respected.

2. eKare inSight - The Solution

How it works?

eKare inSight® is a solution that allows specialist expertise to be accessed quickly and easily when it comes to treating wounds. This is how it works: healthcare providers are equipped with a mobile device with a built-in camera that takes a full 3D measurement of the wound and tissue composition within a few seconds. These images are transmitted to a central server over a secure connection, allowing the specialist to see the images almost immediately (depending on the network speed). This ensures that proper treatment for wounds can be delivered faster, which can prevent complications and shorten treatment processes.

How the solution is structured:

eKare inSight is a medical software compatible with both iOS and Android mobile platforms. inSight software works with the native cameras of the mobile device, as well as the sensor attachment (for the 3D capability), to deliver wound dimensions and wound bed classification.

The data that is collected using the mobile device is stored on the central inSight server in Frankfurt. End users can view the data from the central server and manage it using the SPD digital platform. If desired, the data can be sent to an end user's system

Licensing model:

eKare inSight provides software-as-a-service (SAAS).The end user pays a monthly license fee for the EKare inSight application and for hosting the digital platform on the server in Frankfurt. Where applicable, the user purchases the 3D sensors separately.

Categories of personal data:

eKare inSight is used in healthcare to process personal data for medical purposes. This data falls under special categories of personal data, pursuant to Article 9 of the General Data Protection Regulation. Special categories of personal data are classed as having an 'increased risk'. This means that additional technical and organizational measures should be implemented to ensure data security. Section 3 of this white paper explains in detail what security measures are incorporated into eKare inSight

Stakeholders

eKare Europe BV - is the supplier of eKare inSight in Europe. The EKare inSight server environment in Frankfurt is made available to end users by EKare Europe B.V. as the host. EKare Europe B.V. manages the data. Personal data is processed within inSight in that capacity, but it is not stored outside Europe.

eKare Europe has appointed a Data Protection Officer (DPO) to oversee proper compliance with the GDPR and coordinate with the DPO of healthcare institutions using inSight.

EKare Europe BV
Lireweg 74B
2153 PH Nieuw-Vennep
Nederland

eKare Inc. - is the developer of inSight, and provides upgrades and updates in that capacity. eKare does not have independent access to the server in Frankfurt..

eKare Inc.
Global Headquarters
8280 Willow Oaks Corporate Drive Suite 600
Fairfax, VA 22031, USA

Amazon Web Services Cloud – is the host of the eKare central server in Frankfurt, Germany. This cloud service is fully compliant with the GDPR and falls under the supervision of the Luxembourg Data Protection Authority (Commission nationale pour la protection des données).

Amazon Web Services, Inc.
410 Terry Avenue North
Seattle, WA 98109, USA

Amazon Web Services is certified to the following standards:

- ISO 27001 (information security)
- ISO 9001 (Quality standard)
- ISO 27017 (Information security aspects of cloud computing)
- ISO 27018 (code of practice that focuses on protection of personal data in the cloud)

Furthermore, Amazon Web Services complies with the German Cloud Computing Compliance Controls Catalog (C5), an assessment sponsored by the German government, which was introduced in Germany by the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) to help organizations ensure operational security against regular cyber attacks within the framework of the security. Recommendations for Cloud Providers.

Current certificates and reports can be found at https://aws.amazon.com/compliance/programs

3. eKare inSight & data security

Data security from a privacy law perspective simply means that personal data is protected in three fields

1. CONFIDENTIALITY - This means that personal data is protected as best as possible. Measures must be designed to ensure that personal data is only accessible to those for whom the data is intended.

2. AVAILABILITY - Personal data needs to be available. If personal data is unavailable when needed, this is considered a security breach.

3. INTEGRITY - Personal data must be correct. Working with incorrect data in healthcare can sometimes have fatal consequences.

These three pillars form the basis for protecting not only personal data but all data processed within eKare inSight.

As a result, the eKare inSight data security policy is based on the NEN 7510 standard. This section explains what measures eKare in Sight has implemented to help ensure confidentiality, integrity, and availability as best as possible

CONFIDENTIALITY

One of the most important aspects of data security is that data is accessible only to those persons for whom it is intended. This is known as confidentiality. This means that data should be stored and accessed securely. Transferring data between various environments must also be done so securely. In addition, it is important that control mechanisms are designed to ensure that no data breach has occurred and security measures are fit for purpose.

Measures relating to STORAGE:

All databases within eKare inSight are encrypted. This includes backups.

The iPad as the mobile device is fully encrypted by default. The eKare inSight application is installed using container-based architecture. This protects the data within the inSight environment from other applications, such that a data breach becomes virtually impossible in the event of loss

When connected to the internet, data is stored on the mobile device for a very limited time, because the data is uploaded to the EKare central server in real time. If the mobile device is not connected to the internet, the data is encrypted and stored in the cache until the connection is restored. The mobile device can be used in offline mode, in which case the data remains encrypted in the cache.

The servers in Frankfurt and the digital platform are equipped with dedicated firewalls.

Each organization has its own dedicated part of the server, so organizations cannot access each other’s data.

Measures relating to TRANSFER:

Data transfers between the mobile device and the digital platform/central server are fully encrypted.

Desktop sessions using the online web platform are secured by https.
When using the online platform, no data is stored on the device itself.

Measures relating to ACCESS:

TWO-FACTOR AUTHENTICATION – There is two-factor authentication both when accessing the iPad with the eKare inSight application and logging in to the digital platform. In addition to the usual username password combination, a fingerprint is also required on the mobile device.

IDENTITY MANAGEMENT – eKare provides an administrator account, allowing users to be authenticated

ROLE BASED ACCESS CONTROL (RBAC) - This is fully configurable by the administrator at the customer's end. Each organization can define who has access to specific files.

PASSWORD RULES – The default rule is eight characters (uppercase letter, lowercase letter, digit, and symbol). This can be configured if desired.

Control mechanisms:

Logging – eKare provides an administrator account, which can be used for auditing purposes to check how logging on the basis of audit trailing is used.

Mobile Device Management – If the end user uses a mobile device management solution, this can also be used to remotely manage/protect eKare inSight mobile devices.

The server in Frankfurt, which the digital platform uses, is regularly audited by independent third parties. For more information, see: https:// aws.amazon.com/compliance/programs.

The security software is always updated to run the most recent version.

AVAILABILITY

BACK-UP DEVICE – Data on the mobile device is constantly synchronized with the server in Frankfurt. If the device is not connected to the internet, the data is stored in the device cache until the connection is restored. If the device is offline for more than 48 hours, there may be problems with synchronization and data could be lost from the cache.

Recommendation: synchronize at least every day, preferably using a stable Wi-Fi or 4G connection with an upload speed of 5 Mbps

BACK-UP SERVER – A full backup of the production environment is created every night. Snapshots are also used several times a day as a back-up mechanism.

Since the data is encrypted, backups are also encrypted

REDUNDANCY – Systems are redundant in order to minimize data loss.

INTEGRITY

When sending the data, integrity is protected by network protocols (Transmission Control Protocol or TCP) that are built specifically for this purpose. Data packets that are corrupt or lost are just sent again until the correct receipt is confirmed by the network node to which they are sent (final destination).

4. Management

eKare Europe is responsible for the support and for part of the management of the application. In that capacity, it is technically possible that eKare Europe has access to personal data processed by the inSight environment.

To ensure confidentiality, eKare Europe has implemented the following measures

PROCESSING AGREEMENT – eKare acts as a Data Processor as defined by the GDPR. EKare B.V. has entered into a processing agreement with all Data Controllers (end users) who have provided their consent. If Data Controllers do not have a processing agreement template, the can use the template created by eKare Europe B.V

NDA – eKare Europe B.V. has signed a Non- Disclosure Agreement (NDA) with all its employees. An NDA has also been signed with all end users/ healthcare institutions, in which eKare and its staff are bound by confidentiality..

LOGGING – All administrator activities are logged and can be viewed on request

DATA SECURITY POLICY – eKare inSight has implemented a data security policy based on the NEN 7510 standard.

5. Data breaches

eKare has appointed a Data Protection Officer (DPO) who, in the event of a data breach, acts on behalf of eKare inSight and performs any actions towards any Data Controllers affected (end users of eKare inSight).

eKare inSight has a policy of reporting data breaches on the basis of the requirements laid down by the GDPR. This ensures data breaches can be followed up efficiently and cooperation with the Data Controllers always runs smoothly. eKare inSight maintains a register of data breaches, in accordance with the requirements of the GDPR.

If an institution (end user) suspects or finds that a data breach has occurred, this may be reported to the Data Protection Officer appointed by eKare in Sight, who will launch an investigation. The findings will be shared with the institution.

Tackling and recovering from data breaches is the top priority for eKare inSight, which means that actions in this regard take priority over all other ongoing matters.

6. Data minimization

RESTRICTED COLLECTION – eKare inSight can precisely determine which fields should be present. The institution itself determines which data may and may not be collected.

RESTRICTED STORAGE – No data is stored on the mobile device because data is encrypted and continually uploaded to the EKare central server. If the mobile device is not connected to the internet, the data is encrypted and stored in the cache until the connection is restored. When using the web portal, data remains on the eKare inSight server. This complies fully with the GDPR requirements on data minimization.

RETENTION PERIODS – Data can be automatically destroyed after a specified retention period.

If the healthcare institution opts not to use the eKare central server, data is destroyed from the server once it has been transmitted through it.

If the healthcare institution does opt to use the EKare central server, the data is destroyed or anonymized after the agreed retention period. Data may be destroyed earlier at the request of a client of the healthcare institution.

Personal data may be anonymized for pseudonymized after the retention period, e.g. for research purposes.

7. Other matters

OBTAINING CONSENT – Consent can be obtained from the Data Subject (the patient) through a digital signature on the mobile device.

This may involve the use of third parties, in accordance with the Act on the Additional Provisions for Processing Personal Data in Healthcare and the GDPR.

PRIVACY POLICY – eKare Europe B.V. has implemented technical and organizational measures on the basis of its privacy policy in order to protect the privacy of personal data within its systems and solutions.

8. What you need to do yourself?

The GDPR requires organizations that process personal data (institutions that use eKare inSight) to adopt sufficient technical and organizational measures for the benefit of data security and privacy protection. Technical measures and systems are those that are used in the processing of personal data.

Organizational measures are the operating instructions, namely how employees use resources and systems to process personal data. As a user of eKare inSight, you are largely relieved of the responsibility to implement technical measures to ensure compliance with privacy legislation. However, despite all the measures taken by

eKare, it is important for end users to know how data is processed in compliance with privacy legislation. End users are therefore required to train their employees and set up the necessary processes.

eKare Europe BV | www.ekare.eu