Statement of the Conference of Independent Data Protection Authorities

Federal and state governments of April 29, 2021

Technical data protection requirements for messenger services in the hospital sector

Messenger services have paralleled the proliferation of smartphones in recent years gained central importance for the exchange of messages over the years, other Communication services such as e-mail or SMS are often replaced and count in everyday private life the most popular forms of communication.

Reasons for this are in addition to the usability at any time via smartphone and the ease of use of the range of functions, which allows, in addition to text messages also exchange pictures, videos or voice messages, voice and video calls to be carried out and optionally with individual participants or to communicate in the group. In addition, it is often a matter of free usable offers.

Due to the widespread and established use in the private sector, these messenger services are also increasingly used in the health sector, often associated with the use of a private end device1,2,3.

The professional or commercial use of messenger services is subject to legal chen data protection requirements, which common messenger services have not yet or correspond only to a limited extent. In particular, the widely used service WhatsApp leads in a business use to a number of problems4, the use in largely exclude the hospital. The same applies to others in the private sector frequently used services.

With a view to the sensitivity of the data concerned in the health sector and the special protection that this according to Art. 9 General Data Protection Regulation (GDPR) enjoy, are therefore important when selecting suitable messenger services for the transmission

of patient data in the hospital area by the responsible

relevant data protection requirements to be taken into account. The pro-

at the same time serve as orientation for the use of messenger services

in the established area.

1 https://www.aerztezeitung.de/praxis_wirtschaft/datenschutz/article/902262/klinik-jeder-dritte-arzt-verschickt-patienten-data-via-apps.html

2 https://www.kardiologie.org/kardiologie/whatsapp-und-co--wissen-aerzte--was-sie-tun-/15742284

3 https://deutsches-datenschutz-institut.de/wp-content/uploads/2018/05/FAZ_Messenger-2018.pdf

4 https://www.datenschutz.rlp.de/de/themenfelder-themen/whatsapp/

The use of messenger services in the hospital sector can be

various scenarios (e.g. internal hospital use, consultation, communication

with emergency services, communicating with medical practices, communicating with others

service providers, communication with patients). Depending on the scenario

rio can result in different requirements. The following

Requirements require the use of business end devices and do not include

the use of private devices by employees. The scope of the

Paper extends to communication in the hospital - communication

with external third parties and patients is not affected.

The following requirements relate primarily to the actual measuring

closer application, communication between the participants

users, the platform used and the end devices used. The actual

operation of messenger services in the hospital is only considered insofar as

than general requirements. Not to be considered in this

Due to the heterogeneity of the conditions of use, paper has functional requirements

hospital operations, including the required technical and organizational

safety precautions.

"Significant risks", as formulated in the General Data Protection Regulation5, are

the processing of data categories mentioned in Art. 9 DS-GVO, such as health

data or genetic data, always to be assumed. The need for protection lies in

the personal data itself. If in this paper the processing in a

is addressed to a hospital, it is because the data protection regulations

Requirements are fundamentally addressed to "the" person responsible (in the sense of Art. 4 No. 7 DS-

GMO) and in hospitals i. i.e. R. always involves extensive processing

processing of personal data takes place.

Insofar as the following text formulates mandatory requirements, these are data

required by intellectual property law and must therefore be implemented as a matter of urgency. target

Demands, on the other hand, can have different characteristics: If there are

If there are equivalent alternative courses of action to ensure data protection, it is sufficient

out if one of these is realized. It remains with the person responsible

Within the framework of Art. 24 Para. 1, 25 Para. 1 and Para. 2, 32 Para. 1 DS-GVO

leeway as to which of the options he actually chooses. About it

In addition, should-requirements can, from a data protection point of view

describe a circumstance that is desirable but not mandatory from a legal point of view.

In this case, the person responsible decides whether to comply with the requirement. In the

As a result, the person responsible must ensure that the respective processing

5 See recital 51 sentence 1 GDPR.

is supported by a messenger service, a protection appropriate to the risk

level.

I. Messenger Application

1. The application must offer the possibility to

According to Art. 13 DS-GVO on the data processing associated with the use

to teach. The information must be in a clearly identifiable area

(e.g. information on data protection, data protection declaration) for the at any time

access to be deposited.

2. The application must have the ability, use and access

to the data processed via it to its own prior authentication

(e.g. PIN, fingerprint). This can be based on the operating system radio

functions, but must opt out of the protection for unlocking the mobile

device (see item III. 1).

3. The application must be able to display contact data from communi-

nication participants in their own, from the general

separate address book of the end device used (smartphone, tablet, PC, etc.).

to store memory. You should have a possibility in this regard

import contacts and related information from other sources.

to be able to. You must still have the ability to send messages

as well as file attachments such as images, videos, documents, etc. exclusively in one

own, from the general memory areas of the device used

separate memory in encrypted form. This can be done on the operating system

cryptographic functions available on the tem side can be accessed. The

Application should have the ability to send messages and file attachments

import from other sources.

4. The application should offer the possibility for server-side authentication

tion, encryption or digital signature (e.g. certificates,

key) to import. A communication via the messenger application

may only be used on the basis of reliable identification and authentication

tion of the communication partners may be possible.

5. If electronic signatures or other electronic certificates are used,

there must be a certificate management. In particular, it must be ensured

that electronic keys or certificates clearly belong to a legal entity

son (here: the hospital) or assigned to a natural person and regularly

moderately checked for validity. Compromised keys or certificates

kate must be able to be disabled. It is irrelevant whether the

used Public Key Infrastructure (PKI) operated by the person responsible or by

is made available to a third party.

6. In view of the hospital and professional documentation requirements

and with regard to the fulfillment of data subject rights, the backend must have

have an interface that allows them to be integrated into IT structures and processes

hospital (e.g. uploading security profiles or default

positions, synchronization with the hospital information system, takeover

treatment-relevant messenger messages as part of the patient documents

mention).

7. The application must be able to use the data it manages

delete data specifically or generally (messages, files, contacts, etc.). She

should be able to set a deadline after which such dates

be automatically deleted.

8. Insofar as the use of the application includes third-party error analysis services

are integrated (e.g. Crashlytics), this must be clearly displayed and

be marked as optional; those for a transmission for troubleshooting

intended data categories must be clearly identifiable. A corresponding

Data transfer must be disabled by default. It must be

ensure that data subject to medical confidentiality or data about the

Usage behavior of Messenger users, in this way not unauthorized of-

be revealed.

9. With a view to the availability of the data in accordance with Article 32 (1) (b) GDPR

the application about the possibility of a backup and feasible re-

Production of the relevant contact data/content data/communication processes

feature. Insofar as the storage is carried out in compliance with Art. 28 DS-GVO by a

is taken over by a service provider who does not meet the requirements of Art. 9

Para. 3 DS-GVO, it must be possible to use the data according to the status

to encrypt the technique before its delivery in such a way that a decryption

is only possible with a key that is not disclosed to the service provider and

is secured separately.

A backup to ensure availability from data protection

legal reasons to delimit the storage for documentation purposes

Zen. The relevant medical documentation obligation from a professional law perspective

(cf. § 10 MBO-Ä, § 630f BGB) remains unaffected; she may in a mission

are not neglected by messenger services. A documentary that

(Partly) done in Messenger and not included in the patient documentation

enforceable must be avoided. Treatment-relevant content data that

relate to patients and are generated on the end device

(e.g. by camera recordings), the IT structure of the hospital must

stores and can be found via the treatment documentation, insofar as this is possible

is required from a professional or civil law perspective. For this it is not necessary

a special function adapted to the HIS in the messenger

Application, as long as the process can be mapped efficiently elsewhere. default

The principles of professional and civil law remain untouched.

10. If images are sent via the application (e.g. patient

took, screenshots) in which personal data contained therein for

are not necessary for the intended purpose from a medical point of view, and the patient

ten identity against the background of careful treatment as an exception

is dispensable, there should be the possibility of blackening parts of the recordings

or otherwise excluded from the presentation (data minimization, cf. Art. 5

Paragraph 1 lit. c, 25 Paragraph 1 DS-GVO).

11. The responsible hospital and possibly

to provide the commissioned processor with suitable evidence that

that necessary for the fulfillment of the data protection principles and the guarantee

the security of the processing according to Art. 25 Para. 1 and 32 DS-GVO

functions have been effectively implemented and in the respective processing

processing procedures complied with the requirements of the General Data Protection Regulation

(e.g. certification according to Art. 42 DS-GVO, certification according to European

Privacy Seal, BSI basic protection certification or similar). on the part of

hospital, the messenger application should also be based on the test catalogue

on technical data protection at Apps6 evaluated and the result within limits

of accountability (Article 5 (2) GDPR).

12. The application must comply with Art. 25 Para. 1 DS-

GMO and with regard to their configuration settings the principle of data

correspond to protective default settings (Art. 25 Para. 2 DS-GVO).

13. The application should have (semi) automatic update procedures7.

II. Communication

1. The confidentiality and integrity of the medical

chinic communication must take into account the state of the art

via end-to-end encryption between individuals or groups

of communication participants or the respective

services are guaranteed (Art. 32 Para. 1 lit. a DS-GVO).

2. As far as the integrity of the data communicated via the messenger service for

subsequent measures is important, should there be the possibility

these through cryptographic functions, taking into account the status of the

6 https://www.lda.bayern.de/media/baylda_pruefkatalog_apps.pdf

7 Upcoming updates must be automatically checked daily or at the latest when the app is called up again. The Updates must then be installed automatically or the users must be informed of the existence of an update be informed and can carry out the update with a simple operating step.

Technology to be proven (Art. 32 Para. 1 DS-GVO). Furthermore, to guarantee

tion of the integrity of the information when used for subsequent actions

is important, care is taken to ensure that all data communicated

arrive at the recipient. If a message is

tens of a messenger distributed over several messages (e.g. because the messenger

only allows a certain number of characters or file size per message).

Mechanisms must be integrated that inform the recipient

whether the message sent has arrived in full or whether individual messages

correcting parts are missing. This can e.g. B. by automatically adding a se-

number (“part x of y”) so that the recipient

catchers can see whether all the messages have reached him or her.

3. Connection data for the communication conducted via the messenger service

(e.g. communication participants, time, device and

location data) may only be processed for as long and to the extent necessary for

carry out the transmission of the communication or to maintain it

or restoring the security of electronic communications networks and

services or to detect technical defects and errors in the transmission

transmission of electronic communications is required. The communication

ons and metadata may only be used for the defined, own purposes

of the hospital are used. A use for other purposes by the

Manufacturer of the solution or the platform operator (e.g. advertising purposes) is inadmissible

casual.

4. The use of open communication protocols8 (e.g.

XMPP9, Matrix10) to communicate with other messenger

enable services.

III. Endpoint security

1. The end devices used must have effective access protection

(e.g. PIN/passphrase, biometric solutions). The internal memory of the devices

must be protected by encryption so that decryption

Knowledge of the login data required.

2. Only devices may be used whose operating system version

by the manufacturer of the operating system platform (in particular Google or

8 protocols that conform to an open standard as defined by the Free Software Foundation Europe

(https://fsfe.org/freesoftware/standards/def.de.html).

9 Extensible Messaging and Presence Protocol (XMPP) of the IETF, published as protocol standard RFC 6120, 6121 and

6122

light: https://tools.ietf.org/html/rfc6122

10 For specification see https://matrix.org/docs/spec/

Apple) are currently supplied with security patches and in which all such

security patches immediately or immediately after examination and approval

by the institution's own IT security department, to the extent specified

seen, applied. This assumes that the manufacturers of the terminals

any necessary adaptation to the respective device type immediately

take.

3. The end devices must have a Mobile Device Management (MDM) service

or an equally effective measure (configuration specifications/profiles, installation

lation/usage restrictions, localization, remote deletion, etc.)

, which is ensured by a secure configuration of the devices and data transfer

ties the risk

a) the infiltration of malicious code (e.g. via browser vulnerabilities, da-

viewer, operating system platform and interfaces of the device),

b) unauthorized access by third parties to the device itself and to the processed

dead data

minimized, prohibits processing when the operating system of the device

not the ones listed under Item III. 2 features mentioned, the application of

Triggers security patches and updates and the installation of apps

supervised. The service should also, if necessary, provide location and blocking

tion or deletion of the devices as well as a deletion of personal data

allow in case of loss, but with a permanent localization of the owner

can be ruled out.

IV. Platform/Operation

1. Insofar as the messenger service used is a

publicly available telecommunications service i. s.d. § 3 No. 17a Telekom

Communications Act (TKG), this must comply with the applicable specifications

of the General Data Protection Regulation and the Telecommunications Act

, including in particular Section 6 and Part 7 TKG. With regard to compliance

compliance with telecommunications and data protection requirements

to choose from. The conclusion of a contract in accordance with Art. 28 Para. 3 DS-GVO

(see below) is not necessary in this case.

2. It must be ensured that only authorized users participate in a message

exchange can participate. This applies to the communication of a fixed

laid, closed user group (e.g. hospital), as well as for the

Communication with other participants of the messenger

service. This requires a suitable registration process or

Speaking authorization/authentication mechanisms, such as through a

centrally administered identity management system.

3. For the processing activities associated with the use of the messenger service

activities, the need for a data protection impact assessment (DPIA)

according to Art. 35 DS-GVO. In particular, if these processing

activities are extensive, a DPIA must be carried out (Art. 35 Para. 3 lit. b DS-

GMO). Do several hospitals have similar processing activities by

Messenger services are supported, with a similarly high risk, so can a

further DPIA are omitted if a hospital already has one accordingly

DPIA carried out - if necessary after necessary adjustments - "as own"

(Article 35 (1) sentence 2 GDPR).

4. The hospital must regularly check the messenger solution

assessment, assessment and evaluation of the effectiveness of the protection of processing

technical and organizational measures taken

(Art. 24 para. 1 sentence 2, 32 para. 1 lit. d GDPR).

5. The messenger solution should operate both as a service of a service

ters/processors as well as in the technical infrastructure of the health

allow on-premises.

6. Insofar as contract processors are used to operate the process

it must be ensured that these comply with the regulations of the data protection

Basic Regulation and the requirements of Art. 9 Para. 3 DS-GVO

i. V. m. § 203 Abs. 3 StGB as well as other possibly relevant regulations (e.g. crane

house laws). For this purpose, service providers in Germany, the EU

European Union or the European Economic Area can be used

the.

7. A contract according to Art. 28

Para. 3 DS-GVO to close. In view of the sufficient guarantees technically

organizational measures, processing in accordance with the data protection

Basic Regulation and the protection of the rights of data subjects should

the service provider has appropriate evidence (e.g. certification

according to Art. 42 DS-GVO, certification according to European Privacy Seal, BSI basic protection

certification).

8. For the data stored by the service provider as part of the messenger solution

Regular erasure of data must be ensured (cf. Item I.8). personal

Genetic patient data must be stored on the hospital's servers or its

Contract processors (insofar as they comply with the requirements of the basic data protection

regulation - in particular Art. 9 Para. 3 and 28 DS-GVO -, the federal or state

data protection regulations and, if necessary, taking into account specific national

legal, in particular regional hospital regulations

were processed). The temporary storage on the end devices should

therefore kept as short as possible according to the principle of necessity and in

short cyclic intervals from the end device to the intended server systems

be relocated. This also applies to any container solution in the mobile

messenger app.

9. As soon as they are available, security-related updates of the app in particular are

to be released internally and carried out on all devices used.