SUPPORT POOL
OF EXPERTS PROGRAMME

Standardised Messenger Audit

D1 - Frontend Requirements

by Mathieu CUNCHE

Professor at INSA-Lyon, CITI-Lab
Faculty member of the Inria Privatics team

As part of the SPE programme, the EDPB may commission contractors to provide reports and tools on specific topics.

The views expressed in the deliverables are those of their authors and they do not necessarily reflect the official position of the EDPB. The EDPB does not guarantee the accuracy of the information included in the deliverables. Neither the EDPB nor any person acting on the EDPB's behalf may be held responsible for any use that may be made of the information contained in the deliverables.

Some excerpts may be redacted or removed from the deliverables as their publication would undermine the protection of legitimate interests, including, inter alia, the privacy and integrity of an individual regarding the protection of personal data in accordance with Regulation (EU) 2018/1725 and/or the commercial interests of a natural or legal person.

To produce this deliverable the expert worked closely with the BfDI (ie the DE federal SA), which provided significant input and feedback.

Contributors: Thore Hendrikson, Aline Sylla and Nina Zinnhobler

Document submitted in May 2024

Table of Contents

1 Introduction

Successful communication is an important component for collaboration and teamwork within businesses, as well as a big part of everyday life. While messenger services were intended for personal use when they were first introduced, they are now a widely used tool in various contexts. An essential factor in the use of messenger services is the guarantee and assurance of data protection. In Germany and other European countries, the DSGVO compliance of messengers is therefore an important issue. The messenger service must thus protect the data of its user base, ensure control over their data, and delete data in compliance with the law. In addition, the service must keep data processing to a minimum and use the data only for specified, clear and legitimate purposes. In order for data protection authorities to also be able to consistently and comprehensively advise and monitor companies and institutions on the use of messengers, common requirements for the use of messengers and standardized audit methods in line with the GDPR are essential. The stated goal of the SPE project is therefore to develop a test catalog of mandatory, recommended, and optional requirements using the keywords described in RFC 2119, which a GDPR-compliant messenger front end has to meet. This catalog is primarily supposed to support supervisory authorities in their work, but companies may also be interested in this catalog to review and improve on their product.

1.1 Structure of the Project

The Project consists of two documents. D1 - the requirement catalog and D2 - the audit methodology. This Document - D1 - features the list of criteria. It is closely based on the structure and outline of the General Data Protection Regulation (GDPR), so that for the target group (authorities) of the criteria catalog within the scope of the SPE project, an easier orientation to the respective requirements of the GDPR is ensured and a faster and more comprehensive overview of the requirements of the test criteria can be guaranteed. However, not all articles of the GDPR have corresponding requirements in this catalog, since some articles implore a higher level consideration than these requirements can represent. The criteria were developed for the frontend, i.e. for the presentation level and thus the part of the application that is visible to the user community. Some requirements that relate more to the backend can still be found in this document for the sake of completing some thematic fields, but they are labelled as out of scope accordingly.

The requirements within this catalog are formulated in such a way that a distinction is made between MUST, SHULD and MAY requirements of the respective data protection principles. The MUST criteria are mandatory and their implementation must be ensured for GDPR compliance. The implementation of the so-called SHOULD-criteria is strongly desirable, but not as mandatory as the must-criteria. Still, there has to be solid reasoning behind not implementing a should-criterion. The MAY-criteria are the least necessary criteria, serving as a guide for privacy friendly design. If they are not implemented, there is no risk to compliance with the GDPR.

1.2 Terminology and structural elements

1.2.1 Signal Words

The requirements in this catalog are written with the following signal words:

- MUST: The controller must implement a certain property as a mandatory requirement.
- MUST NOT: The application/backend must not under any circumstances whatsoever have a certain property.
- SHOULD: The application/backend must have a certain property, unless it is shown that failure to transpose does not pose a risk to secure operation or implementation is currently not possible due to technical limitations.
- SHOULD NOT: The application/backend must not have a certain property, unless it is shown that implementation does not pose a risk to secure operation.

- MAY: The application/backend may have a certain property whereby a conversion of this property must be indicated by the solution provider.

1.2.2 Requirement types

In addition to the stable requirements for Messenger Frontends, this Document features several requirements, that were considered as being out of scope. Either because they were more akin to good practice examples than stable requirements, or they were applicable only or mostly to the backend of Messenger applications, which is not the focus of this Project. Regardless, these requirements are listed in D1 as they complete the picture of Messenger Frontends, as well as provide starting points for future Versions. They are, however, not included in D2 and don't have a corresponding verification method.

The different requirement types are tagged and colored as follows:

stable - Is considered a requirement. Has a corresponding verification in D2.

extra - Is not considered as a requirement, but as a good practice. Does not have a corresponding verification in D2.

backend - Is not considered as a requirement for this version of the catalog, as it only applies to the backend. Does not have a corresponding verification in D2

1.2.3 Glossary

- controller: the entity providing the messenger service
- frontend: the software running on the user's device to provide the messenger service
- backend: the software running on an infrastructure controlled by the controller
- application: see frontend
- Message: piece of data sent by a user in a conversation that can be composed of text, emojis, links and multimedia content.
- Username: a string of characters that is freely chosen by the user and does not have to be the users' actual name.

2 Requirements for a a GDPR compliant messenger

2.1 Lawfulness of processing (Art. 6 GDPR)

LEG_BASIS_1 - The processor of personal data MUST provide a legal basis for the processing.

2.2 Conditions for consent (Art. 7 GDPR)

CONSENT_1 - The messenger MUST obtain user's consent before collecting or processing any personal data.

CONSENT_2 - The messenger MUST offer the user the possibility to withdraw consent as easily as it is to provide consent.

CONSENT_2.a - The messenger MUST inform the user about practical restrictions regarding the usage of the messenger resulting from consent withdrawal during the withdrawal process.

CONSENT_3 - The messenger SHOULD offer a simple dashboard listing all given consent options.

CONSENT_3.a - The dashboard from CONSENT_3 SHOULD list all possible consent options, even those the user did not provide.

CONSENT_4 - The request for consent MUST be written in clear and plain language.

CONSENT_5 - The request for consent MUST be clearly distinguishable from all other matters.

CONSENT_6 - During the process of providing consent, the user MUST be able to access the privacy policy.

CONSENT_7 - The interface used for requesting consent MUST NOT use deceptive design pattern or any element nudging the user to provide consent.

2.3 Information / transparency (Art. 12/13 GDPR)

2.3.1 Privacy policy

POLICY_1 - The messenger MUST feature a privacy policy.

POLICY_1.a - The privacy policy MUST include the identity and the contact details of the controller and, where applicable, of the controller's representative.

POLICY_1.b - The privacy policy MUST include the contact details of the data protection officer, where applicable.

POLICY_1.c - The privacy policy MUST include the purposes of the processing for which the personal data are intended as well as the legal basis for the processing.

POLICY_1.d - If the processing is based on Article 6(1)f GDPR, the privacy policy MUST include the legitimate interests pursued by the controller or by the third party.

POLICY_1.e - The privacy policy MUST include the recipients or categories of recipients of the personal data, if any.

POLICY_1.f - The privacy policy MUST include where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47 GDPR, or the second subparagraph of Article 49(1) GDPR, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

POLICY_1.g - The privacy policy MUST include the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

POLICY_1.h - The privacy policy MUST include the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability and how to enact these rights.

POLICY_1.i - The privacy policy MUST include, where the processing is based on Article 6(1)(a) or 9(2)(a) GDPR, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

POLICY_1.j - The privacy policy MUST include the right to lodge a complaint with a supervisory authority.

POLICY_1.k - The privacy policy MUST include whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

POLICY_1.l - The privacy policy MUST include the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) GDPR and, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

POLICY_1.m - The privacy policy SHOULD include the name and contact info of the competent supervisory authority.

POLICY_2 - The privacy policy SHOULD be accessible before to the user starts the account creation process.

POLICY_3 - The privacy policy MUST be displayed to the user upon account creation or upon collection of personal data from the user, whichever comes first.

POLICY_4 - The information provided in the privacy policy MAY be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing.

POLICY_5 - The privacy policy MUST be written in the official language or languages of the country in that the service is provided.

2.4 Right to access (Art. 15 GDPR)

ACC_RIGHT_1 - The controller MUST provide a way for the user to obtain a copy of personal data concerning the user.

ACC_RIGHT_2 - If the request to access was made by electronic means, the controller MUST provide the copy in a commonly used electronic format.

ACC_RIGHT_3 - The controller SHOULD NOT provide the copy in a proprietary format.

ACC_RIGHT_4 - The controller MUST provide at least one copy in an human readable format.

ACC_RIGHT_5 - The controller MAY provide the copy in a machine-readable format in addition to a human readable format.

ACC_RIGHT_6 - The controller SHOULD provide the option to download the copy within the application.

ACC_RIGHT_7 - The controller SHOULD NOT request further personal data beyond what is absolutely necessary in order to fulfill the request to a copy of personal data.

ACC_RIGHT_8 - The controller SHOULD identify the user through an authentication mechanism such as the same credentials used by the user to log-in to the messenger service.

2.5 Right to rectification (Art. 16 GDPR)

REC_RIGHT_1 - The controller SHOULD provide a way for the user to rectify inaccurate personal data concerning the user.

REC_RIGHT_2 - The controller SHOULD place the mechanism to start the process to rectify inaccurate personal data concerning the user adjacent to the user profile.

REC_RIGHT_3 - The controller MAY offer a feature to edit messages sent by the user.

REC_RIGHT_3.a - An edited message MUST be clearly indicated as such to all recipients and the sender of the message.

2.6 Right to erasure (Art. 17 GDPR)

2.6.1 Account deletion

ACC_DEL_1 - The messenger application SHOULD offer a mean to delete the account.

ACC_DEL_1.a - The process to delete the account MUST be as easily accessible as the account creation process.

ACC_DEL_2 - Upon activation of the account deletion feature, the deletion of data SHOULD be executed without undue delay.

ACC_DEL_2.a - The messenger MAY feature a retention period no longer than 4 weeks.

ACC_DEL_2.b - The user MUST be informed of the retention period and its duration upon performing an account deletion request.

ACC_DEL_2.c - The messenger MUST feature a process to trigger the deletion without further delay if the user wishes to waiver the retention feature.

ACC_DEL_3 - Upon account deletion all personal data SHOULD be deleted from the user's device.

ACC_DEL_3.a - Upon account deletion all personal data SHOULD be deleted on the backend server.

ACC_DEL_4 - Upon account deletion, the messages and content authored by the user SHOULD be modified to change the author name to a default value.

ACC_DEL_5 - During the account deletion process the application SHOULD provide the user an easily accessible way to perform a backup as in described in 2.12.18.

ACC_DEL_6 - During the account deletion process the application SHOULD provide the user an easily accessible way to perform a data export as described in **??** in order to export all personal data in a structured, commonly used and machine-readable format.

ACC_DEL_6.a - During the account deletion process the application SHOULD provide the user an easily accessible way to perform a direct data transfer to another controller as described in **??**.

2.6.2 Message deletion

Modern messengers often provide a way to delete a message even after it was sent. Depending on the architecture of the messaging service, the controller might be obliged to delete the message from the backend systems as well as from the recipients devices (frontend). This is usually the case if the backend (permanently) stores sent messages and the frontend only provides a live view of the stored messages without storing a permanent copy in the frontend. In addition to manually deleted messages, some messengers feature self-deleting or self-destructing messages.

MSG_DEL_1 - The messenger SHOULD feature an option to delete a message including its metadata authored by the user.

MSG_DEL_1.a - The message deletion feature MAY delete the message for all participants of the conversation in addition to the user.

MSG_DEL_2 - A deleted message MUST be clearly indicated to all participants of the conversation.

MSG_DEL_3 - A self deleting message MUST be clearly indicated to all participants of the conversation.

MSG_DEL_3.a - The remaining time of self deleting message MUST be clearly indicated to all participants of the conversation.

2.6.3 Data deletion

DATA_DEL_1 - The messenger application SHOULD feature an option to delete all data associated with the messenger application from the device.

DATA_DEL_2 - Upon uninstalling the application, all associated data stored on the device SHOULD be deleted.

2.7 Notification obligation regarding rectification, erasure and restriction of processing (Art. 19 GDPR)

NOTIFICATION_1 - The controller SHOULD communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed.

2.8 Data portability (Art. 20 GDPR)

The requirements of this section address personal data concerning the user, which they have provided to a controller. They apply if and only if the legal basis is user consent or the execution of a contract and the processing is carried out by automated means.

2.8.1 Data export

PORT_1 - The application SHOULD feature a functionality to export personal data concerning the user, which they have provided to a controller, in a structured, commonly used and machine-readable format.

PORT_2 - The specification of the format used for the data export MUST be freely available.

PORT_3 - The data exported SHOULD NOT include the contact list of the user.

PORT_4 - The data exported SHOULD include all messages authored by the user.

PORT_5 - The data exported SHOULD NOT include messages not authored by the user.

2.8.2 Data import

PORT_7 - The messenger SHOULD feature a functionality to import personal data in a structured, commonly used and machine-readable format.

PORT_7.a - The functionality to import personal data MUST be offered during the account creation process.

2.8.3 Direct data transfer

PORT_8 - The messenger SHOULD feature a functionality to directly transmit a data export to another controller.

PORT_9 - The messenger SHOULD feature a functionality to directly receive a data export from another controller.

2.9 Data protection by design and by default (Art. 25 GDPR)

DAT_PROTEC_1 - Personal data SHOULD be deleted or anonymised as soon as possible.

DAT_PROTEC_2 - Personal data SHOULD pseudonymised as soon as possible.

DAT_PROTEC_3 - Anonymisation SHOULD be performed according to the state of the art.

DAT_PROTEC_4 - Pseudonymisation SHOULD be performed according to the state of the art.

2.9.1 Identifiers

IDENTIFIER_1 - The messenger application SHOULD NOT use persistent identifiers of the device.

IDENTIFIER_2 - The messenger SHOULD NOT use identifiers derived from the technical characteristics of the device. (E.g. fingerprinting)

IDENTIFIER_3 - The messenger application SHOULD use identifiers that are specific to the application.

IDENTIFIER_4 - The messenger application SHOULD use identifiers that are reset upon uninstalling the application.

IDENTIFIER_5 - The messenger application SHOULD offer the user an option to reset the used identifiers.

2.9.2 Privacy settings

SETTINGS_1 - Parameters associated with management of personal data SHOULD be grouped in a dedicated section or menu. [CNI18, 11.5]

SETTINGS_2 - The controller MAY choose to offer the user the option to configure the privacy settings and preferences during the account creation process.

SETTINGS_2.a - Privacy settings that are configurable during the account creation process MUST feature the most privacy friendly preset.

SETTINGS_3 - The privacy settings SHOULD be accessible anytime after the account creation/registration.

SETTINGS_4 - All privacy settings MUST be set to most privacy friendly setting by default.

2.9.3 Online status

Most messengers feature an online status of contacts and communication partners. While this feature is often seen as a convenience feature, it must be handled with care since it also offers an easy way for profiling.

ONST_1 - The visibility of the online status SHOULD be configurable by the user.

ONST_1.a - The online status MUST initially be set to be only visible to the user and nobody else.

2.9.4 Read status of messages

Most messengers feature an indicator if a message was received or read by the communication partner. While the confirmation of receipt is less critical, the read status is even more so.

READ_1 - The messenger SHOULD offer a way for a user to configure the visibility of the read status of messages the user received.

READ_1.a - The visibility of the read status of a message MUST initially be disabled.

READ_2 - The messenger SHOULD offer a way to modify the read status of a message the user received.

READ_3 - The signaling regarding the read status of messages SHOULD be processed and handled in the frontend of the recipient.

2.9.5 Typing indicator

Messengers may feature a typing indicator so that the communication partners are able to tell if the correspondent is currently typing or not. While this feature is often comprised as a convenience feature, it must be handled with care as it also offers an easy way for profiling.

TYPE_1 - The messenger SHOULD offer a way for a user to configure the visibility of the typing indicator to other users.

TYPE_1.a - The visibility of typing indicator MUST initially be disabled.

TYPE_2 - The signaling regarding the typing indicator SHOULD be processed and handled in the frontend of the sender.

2.9.6 Profile data

Profile data includes elements related to the user account such as username, profile description, picture, position, location or status.

PROF_1 - The visibility of the profile SHOULD be configurable by the user.

PROF_1.a - The messenger MAY offer to configure the visibility of each profile related information such as profile description, picture etc. individually.

PROF_1.b - If the messenger offers a way to configure visibility settings individually, there MUST be a setting to set the visibility for all profile related information in a single setting.

PROF_2 - The profile MUST initially be set to be only visible to the user and nobody else.

PROF_3 - The messenger SHOULD feature an option to set the elements of the profile to a default value.

2.9.7 Link preview

Some messengers feature an option to display a preview of the website from links the user has received. While this feature is often comprised as a convenience feature, it must be handled with care as it also offers an easy way for profiling.

PREVIEW_1 - The messenger SHOULD feature a way to enable or disable the link preview feature.

PREVIEW_2 - The link preview feature SHOULD initially be disabled.

2.9.8 Multimedia content metadata

METADATA_1 - The messenger SHOULD offer the feature to strip the metadata from multimedia content before sending them.

METADATA_2 - The feature to strip metadata from multimedia content before sending SHOULD be enabled by default.

METADATA_3 - The messenger SHOULD inform the user before stripping metadata from multimedia content.

2.9.9 Communication with other applications

SHARE_1 - Prior to sharing personal data with other applications running on the device the messenger application MUST acquire consent.

2.9.10 Access control to device resources

An application may access device's resources: sensors, data, ... Access to those resources is usually controlled via permissions.

PERM_1 - The messenger application MUST only request individual permissions to access resources from the device that are necessary for the delivery of its declared functionalities.

PERM_2 - The description of the messenger application SHOULD declare the permissions that the application might request at runtime.

PERM_3 - For each requested permission, the messenger application MUST inform the user of the necessity of the permission requested.

PERM_4 - The messenger application MUST NOT circumvent permissions restrictions. (Ex.: using Wi-Fi/Bluetooth permission to infer geolocation).

PERM_5 - The messenger SHOULD request access to a resource only when a feature requested by the user requires the access to the resource.

PERM_6 - The messenger SHOULD request only one permission at a time.

PERM_7 - When requesting access to a resource, the messenger MAY offer a way to remember the choice of the user and apply it to all future requests.

PERM_8 - In case the user refuses to grant access to a resource, the messenger SHOULD continue to work, potentially in a degraded mode.

2.9.11 Application behaviour

APP_BEHAV_1 - The messenger MAY feature a mechanism to blank the display of the current application state while switching between applications.

APP_BEHAV_1.a - The feature to protect the application screen while switching between recent applications SHOULD be enabled by default.

APP_BEHAV_2 - The messenger MAY feature a protection against screenshot capture.

APP_BEHAV_3 - The messenger SHOULD offer the option to lock the application with an individual code, passphrase or device feature.

APP_BEHAV_3.a - The messenger MUST NOT solely use device features in order to provide the feature.

APP_BEHAV_4 - The messenger MUST offer the option to lock the application with an individual code, passphrase or device feature if the messenger is primarily intended to be used with Art. 9 GDPR Data.

APP_BEHAV_5 - The messenger SHOULD NOT display personal data if the user has not requested it.

APP_BEHAV_6 - While running in the background, the messenger application SHOULD NOT collect data other than those strictly necessary to the messenger functionalities.

2.9.12 Identity manager

ID_MGR_1 - The messenger SHOULD offer account creation independent of third party identity managers.

ID_MGR_1.a - The messenger SHOULD offer a login process independent of third party identity managers.

ID_MGR_2 - The messenger SHOULD offer a way to anonymously create an account.

2.9.13 Push notifications

Messengers often feature push notifications in order to quickly inform users about new messages or other events within the application. Although push notifications bear may benefits, the underlying technology often involves third parties and introduces other risks with regard to personal data.

PUSH_1 - Push notifications MUST be configurable by the user.

PUSH_1.a - The push notification MUST initially be disabled.

PUSH_2 - The contents of the push notification displayed SHOULD be configurable by the sending user.

PUSH_3 - The contents of the push notification SHOULD be configurable by the receiving user.

PUSH_4 - The controller MUST prove that the used push notification service complies with the GDPR.

2.9.14 Contact matching

Finding other users within the messaging application is an important part of using a messenger. Still, the handling of the contact information should be done with some considerations in mind.

CONTACT_1 - The controller MUST provide a valid legal basis for processing contact data obtained from the user.

CONTACT_2 - The messenger application SHOULD NOT send a copy of the contacts from the contact book to the backend server.

CONTACT_3 - The contact identifiers sent to the backend server SHOULD be encoded in a way that feature brute-force protection.

CONTACT_4 - The messenger SHOULD offer the option to store individual contacts in the messenger without forcing the usage of the device contact list.

CONTACT_5 - The controller SHOULD implement mechanisms that reduces the risk of exposure of contact lists during contact matching.

2.9.15 Groups

Besides simple direct messaging between two individuals, group messaging between various users is also an important messaging feature. Due to the nature of chatting with multiple communication participants instead of on-one-on communication, this feature bears distinct risks that sometimes require specific solutions.

GROUPS_1 - A user's personal information SHOULD NOT be visible to other users in this group who do not already know the users personal information.

GROUPS_2 - The application SHOULD feature an option for the user to prevent other users from adding them to a group.

GROUPS_2.a - By default, the setting to configure if another user can add them to a group SHOULD be set in a way that this is disabled for all other users.

GROUPS_3 - Prior to being added to a group the user SHOULD be asked for consent.

GROUPS_3.a - The messenger MAY enable the user to configure who can add them to a group without their consent.

GROUPS_4 - New members of a group SHOULD NOT be able to see previous members of a group.

GROUPS_5 - The messenger SHOULD NOT offer a feature to display the list of recently left members of a group.

GROUPS_5.a - When leaving the group, users MUST be offered the choice not to appear in the list of recently left members of the group.

GROUPS_5.b - Users listed in the list of recently left members of a group SHOULD NOT be listed longer than 72h after leaving.

GROUPS_6 - The groups message history SHOULD NOT be visible to new members.

GROUPS_7 - The visibility of a groups message history to new members MAY be configurable by the group admin.

GROUPS_7.a - This configuration SHOULD initially be set so that the history is not visible to new members.

GROUPS_8 - The messenger MAY offer a feature to display a limited number of past group messages to new members of a group.

GROUPS_9 - Upon leaving a group, the past messages of the user MAY be masked as messages from an anonymous past member instead of appearing with that user's identifier.

GROUPS_10 - The messenger SHOULD offer the option to exit a group without notifying the users of the group.

2.9.16 Communities

Besides group messaging between several individuals, communities offer a unique functionality that introduces new features regarding groups and individuals that differ from simple groups and direct messaging. In contrast to a simple group, a community can include individual users as well as simple groups. Thus, communities introduce a new set of risks and possibilities for the user that need to be addressed.

COMMUNITIES_1 - A users personal information SHOULD NOT be visible to other users in a community who do not already know the users personal information.

COMMUNITIES_2 - The application SHOULD feature an option for the user to prevent other users from adding them to a community.

COMMUNITIES_2.a - By default, the option to configure if another user can add them to a community SHOULD be disabled for all other users.

COMMUNITIES_3 - Prior to being added to a community the user SHOULD be asked for consent.

COMMUNITIES_3.a - The messenger MAY enable the user to configure who can add them to a community without their consent.

COMMUNITIES_4 - New Members of a community SHOULD NOT be able to see previous members of a community.

COMMUNITIES_5 - Messengers SHOULD NOT offer a feature to list recently left members of a community.

COMMUNITIES_5.a - When leaving the community, users MUST be offered the choice not to appear in the list of recently left members of the community.

COMMUNITIES_5.b - Users listed in the list of recently left members of a community SHOULD NOT be listed longer than 72h after leaving.

COMMUNITIES_6 - The community chat message history SHOULD NOT be visible to new members.

COMMUNITIES_7 - The visibility of a community chat message history to new members MAY be configurable by the community admin.

COMMUNITIES_7.a - This configuration SHOULD initially be set so that the history is not visible to new members.

COMMUNITIES_8 - The Messenger MAY offer the feature to display a limited number of past community chat messages to a new user of a community.

COMMUNITIES_9 - Upon leaving a community, the past messages of the user MAY be masked as messages from an anonymous past member instead of appearing with that users identifier.

COMMUNITIES_10 - Messenger SHOULD offer the feature to exit a community without notifying the users of the community.

COMMUNITIES_11 - Users that are members of a group MUST be notified, when that group is added to a community.

COMMUNITIES_11.a - Users that are members of a group SHOULD be given the opportunity to leave the group before being added to the community.

2.9.17 Broadcast

Some messengers feature the use of a broadcast functionality such as broadcast lists. Regardless of the specifics of this feature, there are some risks involved when utilizing broadcasts.

BROADCAST_1 - The list of the recipients of a broadcast SHOULD NOT be visible to other users.

2.9.18 Channels

Distinct to broadcast, a messenger may feature channels, which are a special form of groups, where only select users can send messages, while simple members of a channel only have reading permissions.

CHANNELS_1 - A users personal information SHOULD NOT be visible to other users in this channel who do not already know the users personal information.

CHANNELS_2 - The list of the simple members of a channel SHOULD NOT be visible to other users.

C_3 - The application SHOULD feature an option for the user to prevent other users from adding them to a channel.

CHANNELS_3.a - By default the option to configure if another user can add them to a channel SHOULD be disabled for all other users.

CHANNELS_4 - Prior to being added to a channel the user SHOULD be asked for consent.

CHANNELS_4.a - The messenger MAY enable the user to configure who can add them to a channel without their consent.

CHANNELS_5 - New members of a channel SHOULD NOT be able to see previous members of a channel.

CHANNELS_6 - The messenger SHOULD NOT offer a feature to display the list of recently left members of a channel.

CHANNELS_6.a - When leaving the channel, users MUST be offered the choice not to appear in the list of recently left members of the channel.

CHANNELS_6.b - Users listed in the list of recently left members of a channel SHOULD NOT be listed longer than 72h after leaving.

CHANNELS_7 - The channels message history SHOULD NOT be visible to new members.

CHANNELS_8 - The visibility of a channels message history to new members MAY be configurable by the channel admin.

CHANNELS_8.a - This configuration SHOULD initially be set so that the history is not visible to new members.

CHANNELS_9 - The Messenger MAY offer the feature to display a limited number of past channel messages to a new user of a channel.

CHANNELS_10 - Upon leaving a channel, the past messages of the user MAY be masked as messages from an anonymous past member instead of appearing with that users identifier.

CHANNELS_11 - The messenger SHOULD offer the possibility to send messages in the name of the channel instead of with a users own identifier.

CHANNELS_12 - Messenger SHOULD offer the feature to exit a channel without notifying the users of the channel.

2.9.19 Stories

Some messages offer the functionality to post status updates in the form of pictures or text, that are only available for a limited amount of time. For this functionality there are some considerations to make.

STORY_1 - The messenger SHOULD enable the user to configure who can see their stories.

STORY_1.a - This configuration SHOULD initially be set to the most privacy preserving setting.

2.9.20 Third parties

2.9.20.1 Data transferred to third parties

THD_PTY_1 - Before personal data is transferred to a third party, the messenger MUST inform the user of this transfer.

THD_PTY_1.a - Information provided to the user on the third party MUST include the identity and the contact details of the third party and, where applicable, of the third party representative.

THD_PTY_1.b - Information provided to the user on the third party MUST include the nature of the data being transferred as well as the purposes of the processing.

THD_PTY_1.c - Information provided to the user on the third party MUST include the privacy policy of the third party.

THD_PTY_2 - Before personal data is transferred to a third party, consent MUST be obtained from the user.

THD_PTY_3 - Transfer of personal to a third party SHOULD be done over a secure communication channel.

2.9.20.2 Third party hosting

THD_PTY_HOS_1 - If the application uses a cloud as its backend system, the controller MUST demonstrates that it is compliant with the GDPR.

2.9.21 Spellchecks

When writing text messages there is a reasonable chance that some words are misspelled. Especially in the context of mobile devices with the small touchscreen typos are not uncomon. As a feature, some messengers offer automated spellchecking, auto-correction or auto-filling. Most often these features are provided by the keyboard of the system or through a third party service. Although this certainly has many obvious benefits, there is also the risk of leaking every word typed to a unknown third party, so that the messengers need to take special care regarding the inputmethod.

SPELLCHECK_1 - The spellchecking SHOULD be performed entirely locally.

SPELLCHECK_2 - An external third party spellchecking feature MUST be configurable by the user.

SPELLCHECK_2.a - An external third party spellchecking feature MUST be disabled by default.

SPELLCHECK_3 - Before activating the external third party spellchecking feature the messenger MUST inform the user of the associated risks.

SPELLCHECK_4 - The controller MUST provide a valid legal basis for performing spellchecking through an external third party.

2.9.22 Keyboard

KEYBOARD_1 - The messenger SHOULD check if the input method is a third party keyboard.

KEYBOARD_1.a - If a third party keyboard is detected, the messenger SHOULD inform the user of the associated risks.

KEYBOARD_1.b - The messenger application SHOULD offer the user the usage of a local application keyboard.

KEYBOARD_2 - The messenger SHOULD offer the option to signal the keyboard to disable any data collection beyond what is absolutely necessary to perform the basic input processing, including but not limited to word predictions or model training.

KEYBOARD_2.a - The option to signal the keyboard to disable any data collection SHOULD be enabled by default.

2.9.23 Message translation

The messenger may offer a translation feature. If the translation is not performed locally, the input will likely be sent to a third party that will perform the translation. In doing so, the content may be leaked to unintended recipients.

TRANSL_1 - The external third party translation feature MUST be configurable by the user.

TRANSL_1.a - The external third party translation feature MUST be disabled by default.

TRANSL_2 - Before activating the external third party translation feature the messenger MUST inform the user of the associated risks.

2.9.24 Blocked users

BLOCK_1 - The messenger MAY offer a way to restrict other specific users from viewing/accessing a users profile and/or contact information.

2.9.25 Password protected conversations

In contrast to protecting the entire application with a passphrase or PIN, sometimes protecting individual conversations may also be an option to the user.

PRIV_CHAT_1 - The password SHOULD be requested and verified every time the user opens a password protected conversation.

2.9.26 Direct communications

In a centralized architecture, messages are sent to the backend server that forward them tho their destination. Messages can also be directly sent from the sender device to the receiver device over the Internet or even through an ad-hoc network.

DIRECT_COM_1 - Direct communications MUST be configurable by the user.

DIRECT_COM_1.a - Direct communications MUST be disabled by default.

DIRECT_COM_1.b - The user MUST be informed of the risk of using direct communications before activating the feature.

2.9.27 Network proxy

In some situations traffic from devices can be routed through a network proxy that fulfills special tasks.

PROXY_1 - The network proxy feature MUST be configurable by the user.

PROXY_1.a - The network proxy feature MUST be disabled by default.

PROXY_1.b - The user MUST be informed of the risk of using a network proxy before activating the feature.

2.9.28 Data collection for analytics and crash reports

Offering a service and developing applications for this service is always a moving target and a constant balance between adopting and implementing new features requested by the users and maintaining a solid foundation. Since development is never perfect, the controller often prefers feedback and statistics from their customers. Sometimes crash-reports and debugging information helps in ironing out bugs or identifying errors. But since these reports often include fare more data that is strictly necessary for providing the service initself, collection induces risks that need to be considered and covered appropriately.

ANALYTICS_1 - Analytics and debugging data collection MUST be configurable by the user.

ANALYTICS_1.a - Analytics and debugging data collection SHOULD be disabled by default.

ANALYTICS_2 - The user MUST be informed of the risk of enabling analytics and debugging data collection before activating the feature.

ANALYTICS_3 - Error messages and notifications MUST NOT contain personal data or other sensitive data (such as a keys or authentication token). [fSidI20, O.Source_3]

2.10 Processor (Art. 28 GDPR)

PROCESSOR_1 - The messenger controller SHOULD use processor (third party services / libraries processing personal data) providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

PROCESSOR_2 - For each processor, the messenger controller SHOULD have set a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

PROCESSOR_2.a - The contract set with a processor SHOULD stipulate that the processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

PROCESSOR_2.b - The contract set with a processor SHOULD stipulate that the processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

PROCESSOR_2.c - The contract set with a processor SHOULD stipulate that the processor ...

2.11 Records of processing activities (Accountability) (Art. 30 GPDR)

RECORD_1 - On the backend, the controller MUST maintain a record of the processing associated to the messenger application. This record must include : name of the contact, purpose of the processing, description of categories of data ...

RECORD_1.a - The record of processing MUST include the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer.

RECORD_1.b - The record of processing MUST include the purposes of the processing.

RECORD_1.c - The record of processing MUST include a description of the categories of data subjects and of the categories of personal data.

REC_PROC_1.d - The record of processing MUST include the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations.

RECORD_1.e - The record of processing MUST include, where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards.

RECORD_1.f - The record of processing MUST include, where possible, the envisaged time limits for erasure of the different categories of data.

RECORD_1.g - The record of processing MUST include, where possible, a general description of the technical and organisational security measures.

2.12 Security of processing (Art. 32 GDPR)

2.12.1 General security requirements

SECURITY_1 - The controller MUST implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

SECURITY_2 - Personal data SHOULD be encrypted at rest.

SECURITY_3 - Personal data SHOULD be encrypted in transit.

SECURITY_4 - Technical measures SHOULD be implemented to prevent unauthorized access to personal data processed by the application.

2.12.2 Security of communication

COMM_1 - Personal data transmitted from and to the application MUST be done through a secure communication channel.

COMM_2 - Data transmitted from and to the application SHOULD be done through a secure communication channel.

COMM_3 - Secure communication channels MUST NOT be implemented with obsolete or deprecated protocols.

COMM_4 - Deprecated cipher suites MUST be disabled.

COMM_5 - The application SHOULD only use implementations of secure network protocols that are coming from reliable sources and that are maintained.

COMM_6 - The application SHOULD NOT use an implementation of secure network protocols internally developed by the controller.

2.12.3 End-to-end encryption

E2E_ENC_1 - The messages SHOULD be end-to-end encrypted.

E2E_ENC_2 - The application SHOULD offer a way to verify the public key of a contact.

2.12.4 Secure data transfer security for access right and portability

In the context of the access right and data portability processes, the data transferred from the controller to the subject may be encrypted to ensure its confidentiality during the transfer.

SEC_TRANS_1 - During the process of requesting data in the context of exercising the right to access (2.4), the controller SHOULD offer the user a way to provide an encryption key during the process of requesting the data.

SEC_TRANS_2 - During the process of requesting data in the context of exercise of right to access (2.4), the controller SHOULD NOT offer the user a way to provide a freely chosen passphrase with which the data will be encrypted.

SEC_TRANS_3 - During the process of requesting data in the context of data portability (**??**), the controller SHOULD offer the user a way to provide an encryption key during the process of requesting the data.

SEC_TRANS_4 - During the process of requesting data in the context of data portability (**??**), the controller SHOULD NOT offer the user a way to provide a freely chosen passphrase with which the data will be encrypted.

2.12.5 Certificates and trust anchors

CERT_1 - The validity of the certificates SHOULD be verified by the application.

CERT_2 - The messenger SHOULD NOT use self-signed certificates.

CERT_3 - The messenger MAY limit the list of trusted certificate authorities (CA) to a subset of entities considered trustworthy by the controller.

CERT_4 - The messenger SHOULD use certificate pinning.

2.12.6 Key management and storage

KEY_MGT_1 - Cryptographic keys SHOULD be generated using a secure cryptographic random number generator.

KEY_MGT_2 - Cryptographic keys SHOULD NOT be used for more than one purpose. [fSidI20, O.Cryp_4]

KEY_MGT_3 - Cryptographic keys SHOULD be stored in a secure environment.

KEY_MGT_3.a - Cryptographic keys SHOULD be stored in a secure hardware environment.

KEY_MGT_4 - Cryptographic keys SHOULD NOT be hardcoded.

2.12.7 Cryptography

CRYPTO_1 - The messenger SHOULD use cryptographic primitive, schemes and key lengths corresponding to the state of the art.

CRYPTO_2 - The messenger SHOULD NOT use obsolete cryptographic primitives and schemes.

CRYPTO_2.a - The messenger SHOULD NOT use schemes with output, key lengths and parameters below the following thresholds :

- Symmetric Ciphers : key shorter than 128 bits
- Hash function : output shorter than 256 bits
- MAC (HMAC [RFC2104, ISO9797-2]) : output shorter than 128 bits
- RSA : modulus of shorter than 3072 bits, and exponent shorter than 2^{16} bits
- Finite Field Discrete Log problem (e.g. MODP [RFC3526]) : modulus shorter than 3072 bits and
- Elliptic Curve Discrete Log problem : key shorter than 256 bits
- Pairing : key shorter than 3072 bits

CRYPTO_3 - The messenger SHOULD only use implementation of cryptographic primitives and schemes that are coming from reliable sources and that are maintained.

CRYPTO_4 - The messenger SHOULD NOT use implementation of cryptographic primitives and schemes that have been internally developed by the developer of the application.

2.12.8 Random numbers

RANDOM_1 - All random values SHOULD be generated using a secure cryptographic random number generator. [fSidI20, O.Random_1]

RANDOM_2 - The application MAY obtain random numbers from a source provided by the operating system.

2.12.9 Data encryption & protection

FILE_1 - Files containing personal data or other sensitive data (e.g. keys) on the end device SHOULD be encrypted.

FILE_2 - Files containing personal data or other sensitive data (e.g. keys) on the end device SHOULD NOT be stored in location accessible by other application.

FILE_3 - Personal data or other sensitive data SHOULD NOT be stored in files unless necessary.

FILE_4 - Personal data or other sensitive data (e.g. keys) stored in files MUST be deleted as soon as they are no longer needed.

FILE_5 - Personal data and any other sensitive data SHOULD NOT be stored in cache files.

FILE_6 - File encryption methods used MUST be state of the art.

2.12.10 Secure development & General coding / implementation recommendations

SEC_DEV_1 - All development support options (such as log calls, developer URLs, test methods, etc.) SHOULD be disabled in the production version. [fSidI20, O.Source_7]

SEC_DEV_2 - The controller MUST ensure that no debugging mechanisms remain in the production version.[fSidI20, O.Source_8]

SEC_DEV_3 - During the development lifecycle best practises, state of the art and well acknowledged secure development practices, frameworks or standards SHOULD be followed.[ENI17, R.1]

SEC_DEV_4 - Secure coding standards and practises SHOULD be followed. [ENI17, R.4]

SEC_DEV_5 - Specific security requirements SHOULD be defined during the early stages of the development lifecycle.[ENI17, R.2]

SEC_DEV_6 - During the development, testing and validation against the implementation of the initial security requirements SHOULD be performed.[ENI17, R.5]

2.12.10.1 General coding / implementation recommendations

CODE_2 - User input MUST be checked prior to use in order to eliminate potentially malicious values before processing.[fSidI20, O.Source_1]

CODE_3 - Potential exceptions in the program flow SHOULD be intercepted, handled in a controlled manner and documented.[fSidI20, O.Source_4]

2.12.10.2 WebViews / Javascript

This section only applies to mobile application front-end

WEBVIEWS_1 - `mobile` If the application switches to background mode, it SHOULD remove all sensitive data from the current view (Views in iOS and Activities in Android, respectively). [fSidI20, O.Plat_11]

WEBVIEWS_2 - `mobile` The application SHOULD delete application-specific cookies after exiting. [fSidI20, O.Plat_13]

WEBVIEWS_3 - `mobile` The application SHOULD implement URL whitelisting in the context of Webviews, in order to accept connections to URLs controlled or trusted by the controller.

WEBVIEWS_4 - `mobile` The application SHOULD disable local file and content access in the context of Webviews.

WEBVIEWS_5 - `mobile` Interpreted code that may interact with user input (webviews with JavaScript), MUST NOT have access to encrypted memories or user data, except as strictly necessary to fulfil the purpose of the application.[fSidI20, O.Arch_9]

WEBVIEWS_6 - `mobile` The application SHOULD prevent JavaScript from being active during use of WebView. If JavaScript is indispensable for the implementation of the application, the application MUST reject JavaScript from sources outside the controller's control.[fSidI20, O.Plat_10]

WEBVIEWS_7 - `mobile` The application MUST disable any protocol handlers not needed in WebViews. [fSidI20, O.Plat_12]

2.12.10.3 Web front-end security

WEB_SEC_1 - Web The Web application SHOULD be secured according to the state of the art.

WEB_SEC_2 - Web The Web application SHOULD use HTTP Strict Transport Security (HSTS).[ANS21b, R2]

WEB_SEC_3 - Web The Web application SHOULD NOT store personal data or sensitive data in local databases such as (localStorage, sessionStorage and IndexDB).[ANS21b, Sec. 5.5]

WEB_SEC_4 - Web Session cookies SHOULD NOT be accessible via JavaScript. [ANS21b, R30]

WEB_SEC_5 - Web Cross-site transfer of Session Cookies SHOULD be disabled. [ANS21b, R33]

WEB_SEC_6 - Web Session cookies SHOULD NOT be sent over unsecured communication channels. [ANS21b, R31]

WEB_SEC_7 - Cookies MUST only be set once they are needed.

WEB_SEC_8 - Cookies MUST be deleted as soon as they are no longer needed.

WEB_SEC_9 - Web Session identifier SHOULD not be included in the URL. [Fou21, A07_2021]

WEB_SEC_10 - Session identifier SHOULD be invalidated after logout. [Fou21, A07_2021]

WEB_SEC_11 - Session identifier SHOULD be invalidated after idle timeout. [Fou21, A07_2021]

WEB_SEC_12 - Session identifier SHOULD be invalidated after absolute timeouts. [Fou21, A07_2021]

WEB_SEC_13 - Web Access to web resources SHOULD be denied by default.[Fou21, A01]

WEB_SEC_14 - Web The Web application SHOULD implement protection against Cross Site Scripting (XSS) attacks.[ANS21b, sec. 2.2]

WEB_SEC_15 - Web The Web application SHOULD implement protection against Cross-Site Request Forgery (CSRF) attacks.[ANS21b, sec. 2.2]

WEB_SEC_16 - Web The Web application SHOULD implement protection against Server-Side Request Forgery (SSRF) attacks.[ANS21b, sec. 2.2]

WEB_SEC_17 - Web The Web application SHOULD implement protection against SQL Injection (SQLi) attacks.[ANS21b, sec. 2.2]

WEB_SEC_18 - Web The Web application SHOULD implement protection against Local/Remote File Inclusion (LFI/RFI) attacks.[ANS21b, sec. 2.2]

WEB_SEC_19 - Web The Web application SHOULD implement protection against XML External Entity (XXE) attacks.[ANS21b, sec. 2.2]

WEB_SEC_20 - Web The controller SHOULD monitor Certificate Transparency logs and revoke fraudulent certificates.[ANS21b, R3]

WEB_SEC_21 - Web The Web application SHOULD implement a Content Security Policy (CSP) configured according to the state of the art.[ANS21b, Sec. 5.3]

WEB_SEC_22 - `Web` The Web application SHOULD NOT use code evaluation functions.[ANS21b, 5.2.2]

WEB_SEC_23 - `Web` The Web application SHOULD feature a client-side integrity verification of internal resources.[ANS21b, R11]

WEB_SEC_24 - `Web` The Web application SHOULD feature a client-side integrity verification of external resources.[ANS21b, R12]

WEB_SEC_25 - `Web` The Web application SHOULD implement a Referrer-Policy configured according to the state of the art.[ANS21b, Sec. 5.4]

WEB_SEC_26 - `Web` The Web application SHOULD implement protection against ClickJacking. [ANS21b, R17-18]

2.12.11 Logs

LOGS_1 - The application SHOULD not write any personal data in the logs.

LOGS_2 - The application SHOULD not write any keys in the logs.

LOGS_3 - The logs SHOULD be encrypted at rest.

2.12.12 Third party software

THRDP_SOFT_1 - Third-party libraries and frameworks SHOULD be used in their latest available version for the platform operating system in use. [fSidI20, O.TrdP_1]

THRDP_SOFT_2 - The controller MUST perform regular checks of third-party libraries and frameworks with regard to vulnerabilities. [fSidI20, O.TrdP_2]

THRDP_SOFT_2.a - Functions from libraries and frameworks MUST NOT be used if any vulnerabilities are known.[fSidI20, O.TrdP_2]

THRDP_SOFT_3 - The application SHOULD not disclose personal data to third-party libraries. [fSidI20, O.TrdP_6]

THRDP_SOFT_4 - Before using third-party libraries and frameworks, their source SHOULD be checked for trustworthiness. [fSidI20, O.TrdP_5]

THRDP_SOFT_5 - Data received via third-party libraries and frameworks SHOULD be validated. [fSidI20, O.TrdP_7]

THRDP_SOFT_6 - Third-party software that is no longer kept up-to-date by the manufacturer or developer SHOULD NOT be used.[fSidI20, O.TrdP_8]

2.12.13 Software updates

UPDATES_1 - `mobile` `desktop` The messenger application SHOULD feature a mechanism to allow updates.

UPDATES_2 - `mobile` `desktop` The messenger application SHOULD inform the user when an update is available.

UPDATES_3 - `mobile` `desktop` The messenger application SHOULD verify the integrity of software updates before installation.

UPDATES_4 - `mobile` `desktop` The messenger application SHOULD verify authenticity of software updates before installation.

UPDATES_5 - `mobile` `desktop` For each update related to security, an application that has not been updated SHOULD refuse to work after a grace period. The duration of the grace period SHOULD be based on the criticality of the vulnerability corrected by the update.

2.12.14 Software distribution

DISTRIB_1 - `mobile` `desktop` The controller SHOULD offer to the user a way to verify the authenticity and integrity of the application and updates before installation.

DISTRIB_2 - `mobile` `desktop` The controller SHOULD offer a way to directly obtain the application from the controller.

DISTRIB_3 - `mobile` `desktop` The controller MAY distribute the messenger through third party platforms in addition to direct distribution channels from the controller.

2.12.15 Authentication

AUTH_1 - The messenger system SHOULD enforce a password policy according to the state of the art.

AUTH_2 - The messenger SHOULD provide a way to change the password and other authentication tokens.

AUTH_3 - The messenger MAY feature a second authentication factor.

AUTH_4 - The messenger SHOULD use open standards for a second authentication factor.

AUTH_5 - The messenger MUST NOT use SMS for a second authentication factor.

AUTH_6 - For authentication based on a username and a password, the strength of the password used MAY be displayed to the user. Information regarding the strength of the chosen password MUST NOT be retained in the application memory or backend. [fSidI20, O.Auth_8]

AUTH_7 - `mobile` When credentials are entered via the keyboard, the application SHOULD prevent recordings from becoming visible to third parties. This specifically excludes auto-correction and auto-complete functions, third-party input keyboards and any form of storage that can be evaluated by third parties. [fSidI20, O.Data_9]

AUTH_8 - The messenger SHOULD require a second level authentication before accessing sensitive data or modifying sensitive settings.

AUTH_9 - Suitable authentication and authorisation MUST be provided at the backend interface for connecting a backend system. [fSidI20, O.Auth_2]

AUTH_10 - The backend and the application MUST provide measures to prevent any trying out of login parameters (such as passwords) (e.g. brutefore or dictionnary attacks). This can be achieved, for instance, by delaying subsequent login attempts or by using so-called captchas. [fSidI20, O.Auth_10]

2.12.15.1 Lock / logout

LOCK_1 - The messenger application SHOULD provide a way to logout the user from the messenger service.

LOCK_2 - The messenger application SHOULD provide a way to lock the application.

2.12.15.2 Third party identity services

ID_SERV_1 - The messenger MAY offer to the user the possibility to authenticate through a third party identity service.

ID_SERV_2 - The third party identity service MUST be GDPR compliant.

2.12.15.3 Re-authentication When using a messaging service it might happen, the user does not use the service for long periods of time. To protect the integrity of the service, the controller might decide to request a re-authentication of the user in order to validate, that the user still is the same user who is accessing the service after this long period. With regard to sensitive data stored or processed in the messaging service, the controller may opt for requesting a re-authentication independent of time passed since the last authentication.

REAUTH_1 - The messenger MAY feature a re-authentication mechanism such as a PIN code, a passphrase, or other authentication mechanisms.

REAUTH_2 - The application MAY require re-authentication when it is launched or after a period of inactivity. [fSidI20, O.Auth_11]

REAUTH_3 - The messenger MAY require re-authentication before accessing sensitive data or modifying sensitive settings.

2.12.16 Stateful and stateless authentication

2.12.16.1 Stateful authentication

SF_AUTH_1 - Session handling SHOULD be implemented using secure frameworks. [fSidI20, O.Sess_1]

SF_AUTH_2 - Session identifiers SHOULD be protected as sensitive data. [fSidI20, O.Sess_3]

SF_AUTH_3 - Session identifiers MUST NOT be stored unencrypted on permanent storage media. [fSidI20, O.Sess_4]

SF_AUTH_4 - `Web` The application and its backend SHOULD actively terminate the application session after an appropriate session timeout, according to current best practice recommendations. [fSidI20, O.Sess_5]

SF_AUTH_5 - When an application session is terminated, the application SHOULD securely delete the session identifier in the device. [fSidI20, O.Resi_6]

SF_AUTH_6 - When an application session is terminated, the application SHOULD securely delete the session identifier on the backend. [fSidI20, O.Resi_6]

SF_AUTH_7 - Session identifiers SHOULD be created by the random number generator of the backend. [fSidI20, O.Sess_2]

2.12.16.2 Stateless authentication

SL_AUTH_1 - The authentication token SHOULD be kept in a secure memory area on the device (e.g. KeyChain/KeyStore).

SL_AUTH_1.a - The authentication token in the device SHOULD be protected from easy access by third parties (for example, in the case of rooted/jailbroken devices). [fSidI20, O.Tokn_1]

SL_AUTH_2 - Sensitive data MUST NOT be embedded in an authentication token. [fSidI20, O.Tokn_2]

SL_AUTH_3 - The private key used to sign the authentication token MUST NOT be present in the device. [fSidI20, O.Tokn_5]

SL_AUTH_4 - The messenger application SHOULD feature an option to invalidate all previously issued authentication tokens (for instance, if the device was lost).

SL_AUTH_5 - An authentication token MUST include the fully qualified name of the backend. The application MUST check the fully qualified name. [fSidI20, O.Tokn_3]

SL_AUTH_6 - The backend MUST use a suitable procedure to sign the authentication token (see CRYPTO_X). [fSidI20, O.Tokn_4]

SL_AUTH_7 - The backend MUST check the token. The signature type MUST NOT be none. [fSidI20, O.Tokn_6]

SL_AUTH_8 - The backend MUST reject requests with an invalid or unsigned authentication token. [fSidI20, O.Tokn_7]

SL_AUTH_9 - The backend MUST allow for an appropriate time-to-live when evaluating the validity of a token. [fSidI20, O.Tokn_8]

SL_AUTH_10 - The backend MUST provide the user with existing authentication tokens when requested. [fSidI20, O.Tokn_9]

SL_AUTH_11 - The backend MUST allow the user to invalidate one or all previously issued authentication tokens (for instance, if the device was lost). [fSidI20, O.Tokn_10]

2.12.17 Resilience

RESI_1 - **`mobile`** The messenger application MAY check if the device is rooted / jailbroken and inform the user of the associated risks. [fSidI20, O.Resi_2]

RESI_2 - The application SHOULD reliably detect and prevent the start in a development/debug environment. [fSidI20, O.Resi_3]

RESI_3 - **`desktop`** The application MUST abort its start if it is launched under unusual user rights (for instance, root or nobody). [fSidI20, O.Resi_4]

2.12.18 Backup & recovery

In contrast to the data described in 2.8, a backup can include all kinds of data and is not exclusively reliant on consent or a contract as a legal basis.

BACKUP_1 - Backups SHOULD be encrypted.

BACKUP_2 - The application SHOULD provide a way to create a backup of the data stored locally.

BACKUP_3 - The application MAY offer cloud backups in addition to local backups.

BACKUP_4 - The application SHOULD provide a way to restore the data from a previous backup.

2.12.19 Account recovery

ACC_REC_1 - The messenger SHOULD provide a mean to recover an account in case of a credential loss.

ACC_REC_2 - The recovery mechanism interface SHOULD NOT display if an account is linked to the identifier provided for the recovery.

ACC_REC_3 - Registration, credential recovery, and API pathways SHOULD be hardened against account enumeration attacks by using the same messages for all outcomes. [Fou21, A07_2021]

2.12.20 Security audit

SEC_AUDIT_1 - The provider MUST regularly audit the security of the messenger system.

SEC_AUDIT_2 - The provider SHOULD have a process for regularly auditing the security of the messenger system.

2.12.21 Security certification and adherence to code of conduct

SEC_CERTIF_1 - The controller MAY demonstrate compliance with the GDPR for some or all of these requirements by providing a certificate if it adheres to one or more appropriate and approved certification mechanism as marked down in Art. 42 GDPR.

SEC_CERTIF_2 - The controller MAY adhere to an approved code of conduct.

2.12.22 Illegitimate process

ILL_PROCESS_1 - The messenger controller SHOULD take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless they are required to do so by Union or Member State law.

2.13 Data protection impact assessment (Art. 35 GDPR)

DPIA_1 - The messenger provider SHOULD have conducted a data protection impact assessments before the service is open to users.

DPIA_2 - The messenger provider MUST conduct a data protection impact assessments each time the service undergo a change that significantly changes the processing of personal data.

DPIA_1.a - The messenger provider SHOULD seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

DPIA_1.b - The protection impact assessment SHOULD contain a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller.

DPIA_1.c - The protection impact assessment SHOULD contain an assessment of the necessity and proportionality of the processing operations in relation to the purposes.

DPIA_2.d - The protection impact assessment SHOULD contain an assessment of the risks to the rights and freedoms of the users.

DPIA_2.e - The protection impact assessment SHOULD contain the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

References

[ANS17] ANSSI. Security Recommendations for TLS, January 2017.

[ANS21a] ANSSI. Guide de sélection d'algorithmes cryptographiques. Technical report, August 2021.

[ANS21b] ANSSI. Recommandations pour la mise en œuvre d'un site web : maîtriser les standards de sécurité côté navigateur. Technical report, April 2021.

[CNI17] CNIL. Deliberation no. 2017-012 of 19 January 2017 on the adoption of a recommendation relating to passwords. Technical report, January 2017.

[CNI18] CNIL. Analyse d'impact relative à la protection des données (AIPD) 3 : les bases de connaissances. Technical report, 2018.

[EDP22] EDPB. Guidelines 01/2022 on data subject rights - Right of access. Technical report, January 2022.

[EDP23] EDPB. Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them. Technical Report Version 2.0, February 2023.

[ENI14a] ENISA. Algorithms, Key Sizes and Parameters Report. Technical report, 2014.

[ENI14b] ENISA. *Study on cryptographic protocols.* Publications Office, November 2014.

[ENI17] ENISA. *Handbook on security of personal data processing.* Publications Office, LU, 2017.

[fIS] Federal Office for Information Security. Creating Secure Passwords.

[fIS23] Federal Office for Information Security. BSI TR-02102-1: Cryptographic Mechanisms: Recommendations and Key Lengths. Technical report, January 2023.

[fIS24] Federal Office for Information Security. Standardised messenger audit d1 - frontend requirements. Technical report, 2024.

[Fou21] The OWASP Foundation. OWASP Top 10: 2021, 2021.

[fSidI20] Bundesamt für Sicherheit in der Informationstechnik. Security requirements for eHealth applications. Technical report, 2020.

[GSBM23] Colin M. Gray, Cristiana Santos, Nataliia Bielova, and Thomas Mildner. An Ontology of Dark Patterns Knowledge: Foundations, Definitions, and a Pathway for Shared Knowledge-Building, September 2023. arXiv:2309.09640 [cs].

[IAN23] IANA. Transport Layer Security (TLS) Parameters, September 2023.

[NIS19] NIST. Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. Technical Report NIST Special Publication (SP) 800-52 Rev. 2, National Institute of Standards and Technology, August 2019.

[WP214a] WP29. Opinion 05/2014 on Anonymisation Techniques. Technical report, October 2014.

[WP214b] WP29. Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting. Technical report, November 2014.

[WP217] WP29. Guidelines on the right to data portability. Technical report, May 2017.

European Data Protection Board