IT SECURITY AT MOBILIZE ME APS

A walkthrough for municipalities

Mobilize Me ApS
Åbogade 15, 8200
Aarhus N
Denmark

Table of content

INTRODUCTION	3
IT SECURITY AT MOBILIZE ME APS - FAQ	3
USER ADMINISTRATION	4
SYSTEM OWNER	5
DATA PROCESSING AGREEMENT	5
CHOOSING A PASSWORD	5
PIN CODE PROTECTION OF DEVICES	5
SENSITIVE INFORMATION	6
PERSONAL DATA	6
USE OF PICTURES	6
CONSENT	7
TEXT MESSAGES	7
PROCESS FOR USER DATA ACCESS	7
PROCESS FOR LOST DEVICES	7

INTRODUCTION

This document guides you through some of the security issues, that should be considered, when implementing Mobilize Me ApS' support aids in a municipality. The guide starts by answering some of the questions, that is usually asked by the municipalities. The questions are mostly of a technical kind, and are related to the structure of the system.
Thereafter, we describe which responsibilities should be delegated, before the support aids are implemented. This is primarily about ensuring that someone takes responsibility for the day to day handling of administrative tasks, that are related to the support aid.
Lastly, we describe a series of procedures, that are set in place to help your staff handling the day to day use of the support aids in the best - and safest - possible way. This includes guidelines for daily use of the support aids when it comes to sensitive and personal data.
If you have any further questions, please contact us at: contact@mobilize-me.com

---

IT SECURITY AT MOBILIZE ME APS - FAQ

1. Is user related content stored locally on the tablet/smartphone?
Yes, some local content is stored on the user's device, as experience has shown that there many users have the need to access their data in offline mode. The informations that are cached, are not necessarily personal data, and they are exclusively entered by the users or their support persons. The information is e.g. "Shopping at Tesco" or "Play time with Michael", and images supporting these activities. When the user logs out of the support aid, the cached information is deleted.

2. Is the user's content stored centrally on a server/cloud solution?
Mobilize Me ApS stores the information centrally in a cloud solution on national servers in Denmark. Relevant data are synchronized with the user's device when needed.

3. Are registered personal informations protected in Mobilize Me ApS' security measures, according to the current ISO standard?
Yes, our main supplier lives up to the revised ISO27000 standard, in addition to the Danish Standard for information security (DS484).

4. What are the supplementing technical security measures for personal and sensitive data?
We log all activities at our system - e.g. transaction logging and denied access logging. It is also possible to differentiate user roles and rights, if needed.

5. Do you use strong encryption on open networks?
Yes, all traffic is SSL encrypted.

6. What encryption standard do you use?
We use a 2048 bit encryption key.

7. Who is Mobilize Me ApS' data hosting service provider?
Our provider is Cloud.dk - their security standard is described on the following website: http://www.cloud.dk/da/teknik/sikkerhed

8. Are the informations entered and registered when creating a licence protected by recognized security measures?
Yes, Mobilize Me ApS uses e-conomic, which is a recognized accounting program, which focuses strongly on data security. They follow the Danish Revision Standard RS3000. Their security standard is described on the following website: http://www.e-conomic.dk/regnskabsprogram/sikkerhedteknik/sikkerhed

USER ADMINISTRATION

Local administrator: We recommend that one or more local administrators are appointed and given access to create, disable and edit user profiles. By having local administrators, you ensure that you can react quickly and efficiently in case of unexpected events, such as loss of devices.
Central user administration: If the municipality already uses a central system, it is also possible to do the administration from there. However, it is important to consider who handles the administration, to ensure the staff know who to contact when changes are to be made.
If you want an offer on integration of support aids from Mobilize Me ApS to your existing systems, please contact us.

SYSTEM OWNER

It is important to appoint a system owner, who is responsible for IT security, operation, maintenance and contractual issues with Mobilize Me ApS. The system owner takes responsibility of staying updated on guidelines for use of the support aids and keeping the staff informed on updates, changes etc.

DATA PROCESSING AGREEMENT

Mobilize Me ApS strongly recommends that a data processing agreement is made. By doing so, we take responsibility for the data stored on our servers, and you avoid responsibility of something that is out of your control. We think that makes the most sense for all parts.

CHOOSING A PASSWORD

As in most other systems, it is important that the users change the password into a personal password. This can be done inside the app.
A strong password contains the following elements:
• Is minimum 8 characters long
• Contains both small and capital letters
• Contains numbers
• Contain special characters (&%#)

PIN CODE PROTECTION OF DEVICES

We also strongly recommend that the user has pincode or touch ID activated on their device. If the user loses their device while logged in, a third party will be able to open the app and access the user's data - until the user account is disabled.

SENSITIVE INFORMATION

Mobilize Me ApS' support aids are created to handle sensitive information, but it is not their purpose. We recommend that you don't enter sensitive information into the support aids. Sensitive information includes, but is not limited to:

- Health information
- Criminal records and similar personal issues
- Personality tests
- Racial or ethnical background
- Political, religious or philosophical beliefs
- Sexual preferences
- Major social issues

PERSONAL DATA

In short, personal data covers information, that can be expected to identify or lead to a physical person. It can be identification information, such as name or address, or family background. These are not sensitive informations, but are to be treated with care. We strongly recommend that personal data is not used in the support aids, but limited to information that is related to the user's use of the support aid.

USE OF PICTURES

Pictures are a big part of Mobilize Me ApS' support aids, and an effective instrument to aid our users. However, it is important that the staff considers that sensitive information is not to be included, when taking pictures.
This includes, but is not limited to, images of:

- A medicine bottle, with name and/or social security number printed on it
- A religious journal
- An envelope or document with visible name and address

CONSENT

If it is necessary to take a picture of another person, it is important to get their consent. The person has to be aware that they are being photographed, and it is recommended to get a written consent.

It is allowed to take a picture of a crowd (at a party, a convention or similar), without getting consent, as long as individual persons are not in focus.

TEXT MESSAGES

Generally, the same rules apply to text messages, as for using pictures: Avoid writing about sensitive information and try to avoid using personal information.

PROCESS FOR USER DATA ACCESS

If a user makes a request to their support person, to get access to their user data, the support person contacts the local administrator. They will contact Mobilize Me ApS in writing, and request the relevant data. We deliver the data in a secure mail directly to the user.

PROCESS FOR LOST DEVICES

In case a user loses their device, they or their support persons should immediately contact the local administrator, who can deactivate the user's profile. All the user data stay saved on our server, but it is not possible to log into the user's profile, until it is reactivated.
In case of the device being offline, we can not reach it, and it is therefore possible to access the user's plan, until the device is online again.