NAM SYSTEM
MONITORING TECHNOLOGY

Technologies for monitoring
and protecting assets, vehicles and people

PRIVACY POLICY

HelpCare

V.20180201-

PURPOSE

This document describes the impact of Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, the repealing of Directive 95/46/ES (General Data Protection Regulation) (hereinafter the „Regulation“) and subsequent legislation on the HelpCare system of the company **NAM system, a.s.** with the registered address U Pošty 1163/13, 735 64 Havířov – Prostřední Suchá, Czech Republic, ID: 25862731, registered in the Business Register by the Regional Court in Ostrava, section B, and use of the same.

This document describes the roles, rights and responsibilities of individuals with regard to the personal data of user's clients and employees or other persons relating to the user, with the exception of the user's personal data. Therefore, the user is obliged, in relation to such personal data, to fulfill all obligations laid down for the controller by the law (i.e. the Regulation). However, the user is not a controller with respect to personal data identifying the user as a contract party with the operator, contact details of the user, data describing services provided to the user, payment details and payment history of the user. In relation to such data, the controller is the operator because it has identified the purposes and means of personal data processing. The operator's privacy policy (see "Role: HelpCare User") can be found at www.namsystem.com/gdpr/.

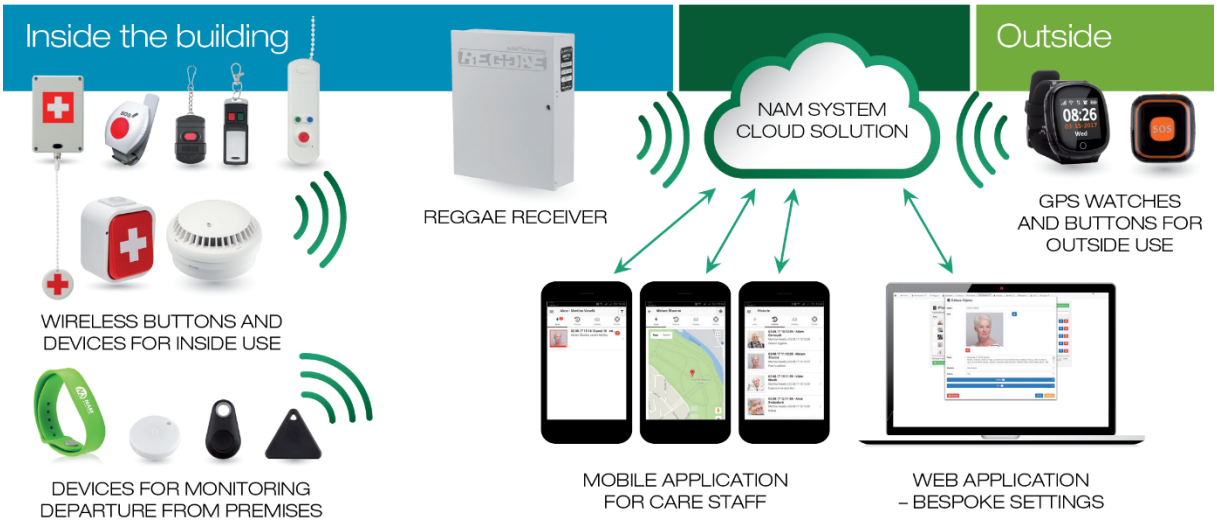
SYSTEM DESCRIPTION

HelpCare is a system for calling help, ensuring people's safety and making staff records. The primary function of the system is to call for help in the event of life-threatening or other restrictive situations. The system also provides an overview of how the situation occurred, when and where it happened and who and how it was resolved.

TECHNICAL SOLUTION

Technically, the system consists of HW and SW parts.

The HW part includes various types of emergency buttons (personal / pocket, bracelet, fixed, buttons with chains, strips, etc.), various designs of environmental detectors (fire detector, flood detector, etc.) and various types of GPS / SOS watches. The hardware section also includes receivers of emergency buttons and detectors "REGGAE GTWbz" that are permanently installed in buildings where the system HelpCare is used and mobile phones of those members of staff responsible for resolving emergency events (medical staff, security guards, etc.). There are no personal data stored in the HW part of the system.



The SW part consists of:

- The HelpCare server application:

  - evaluates all events in the system
  - sets up actions depending on the settings
  - controls the sending of notifications
  - handles mobile application requirements

A web interface is used to administer the HelpCare server application. Since data of users and clients are stored in the HelpCare server application database, the personal data legislation has an impact on the SW part.

- The HelpCare mobile application:

  - is installed on staff mobile phones
  - handles notifications and passes information about emergency situations to the staff
  - displays the data needed to resolve the emergency situation (after confirmation of the event)
  - does not store any personal data of clients locally

PARTICULAR ROLES IN THE HELPCARE SYSTEM

To assess the HelpCare system for compliance with privacy rules, it is appropriate to divide the system into several roles and consider each one separately:

ROLE: HELPCARE OPERATOR

NAM system, a.s. is an operator of the HelpCare system and has developed and manufactured HW parts of the system. In the system, it acts as a technology company and, in terms of the Regulation, it is the so-called "processor". The operator ensures the smooth functioning of the hardware which runs the HelpCare server application and also its security, conducts the administration of individual accounts of system users and provides technical support and training.

ROLE: HELPCARE USER

The user is an organization that uses the HelpCare system and is in a contractual relationship with the system operator. Typically, users are organizations such as retirement homes, hospitals, social offices, business centers and others. The operator creates a separate, isolated account for the user with specific access and administrator rights.

In terms of the Regulation, the user is a controller of the personal data transmitted to the operator by the user or by a third party on behalf of the user or inserted into the HelpCare system by the user or said third party (personal data of clients, employees and others apart from personal data of the user alone). Therefore, the user is obliged, in relation to such personal data, to fulfill all obligations laid down for the controller by the law (i.e. the Regulation).

However, the user is not a controller with respect to personal data identifying the user as a contract party with the operator, contact details of the user, data describing services provided to the user, payment details and payment history of the user. In relation to such data, the controller is the operator because it has identified the purposes and means of processing such personal data.

User / Admin: Using this interface, the user can create additional access to the system with administrator or user rights, define clients with the necessary information, assign emergency buttons, detectors, receiver systems, and set rules for how the entire system should behave for the user. User account administration is performed through the web interface and the user / administrator is also responsible for the security of the computer from which the administration is carried out.

User / Personnel: This is access to the system created by the user/admin. The user / personnel have got very limited rights, these rights allowing them to work with the HelpCare mobile application only to the extent necessary for them to provide assistance in the event of an emergency situation. Via the mobile application, the user/personnel can find the personal data of the client to whom they provided assistance in an emergency situation. Mobile application security is provided at the level of supported versions of the mobile phone operating system and by encrypted communication between the application / mobile phone and the technology center.

ROLE: CLIENT

A person equipped with a panic button or GPS / SOS watch who activates the call for help in an emergency situation. A specific radio signal e.g. from an emergency button, is captured by the receiver in the object/building and transmitted, via a secured route, to the system's technology center. The receivers are equipped with a communicator that uses its own data APN without internet access. The user / client has no access to the HelpCare system.

The client is a data subject within the meaning of the Regulation.

LEGAL ASPECTS OF THE HELPCARE SYSTEM

In terms of the Regulation and other privacy legislation the individual roles and responsibilities are as follows:

CONTROLLER

The HelpCare user is a controller within the meaning of the Regulation and therefore is obliged to perform all the controller´s obligations set forth in the Regulation and other legislation regarding the personal data of clients, employees and other natural persons whose personal data the user has put or has allowed to be put into the system, apart from personal data that the operator is responsible for (see "Role: HelpCare User"). The user is also obliged to allow said data subjects to exercise their rights. Among others, these responsibilities include:

- adhering to the principles of processing personal data,
- providing the data subject with all the information specified in Articles 13 and 14 of the Regulation,
- enabling each data subject to exercise their rights as set out in the Regulation,
- being able to prove that processing was done in compliance with the Regulation and other legislation.

PROCESSOR

The HelpCare operator, i.e. the company NAM system, a.s., is a processor within the meaning of the Regulation.

The relationship between the operator and the user is governed by a contract that is binding on the operator (processor) with regard to the controller (i.e. user) 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 set out in the Article 28 of the Regulation. The contract stipulates, in particular, that the operator processes the personal data only according to documented instructions from the controller (i.e. the controller within the meaning of the Regulation).

The operator does not use any other personal data processor to operate the HelpCare system. If in the future deployment of another processor was necessary, the operator shall do so only with the prior specific or general written permission of the controller (the user) and only under the contract between the operator and the other processor that imposes on that other processor the same data protection obligations as set out in the contract between the user and the operator.

DATA SUBJECT

The data subject in terms of the Regulation is:

- an employee of the user whose personal data are processed in the HelpCare system,
- a client of the user whose personal data are processed in the HelpCare system.

LEGAL BASIS AND PURPOSE OF THE PROCESSING

In relation to employees of the user, the legal basis for processing may be according to the case referred to in Article 6.1 point f) of the Regulation, therefore, that processing is necessary for the purposes of the legitimate interests pursued by the controller. These legitimate interests of the controller may be the

performance of the user´s business because without the use of HelpCare the controller (the user) cannot provide services to his clients to the extent and quality that would be possible if using this system.

In relation to clients of the user, the legal basis for processing may be the case referred to in Article 6.1 point b) of the Regulation, therefore, that processing is necessary for the performance of a contract to which the data subject is party, and if this legal basis is not given in relation to some or all personal data of the client, then the case referred to in Article 6.1 point a) of the Regulation, i.e. the data subject has given consent to the processing of his or her personal data for one or more specific purposes. However, if, in the HelpCare system, personal data belonging to special categories of personal data (client health data) are processed by the controller, the legal basis for the processing can solely be the case referred to in Article 6.1 point. a) of the Regulation, therefore, that the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

The controller shall:

- procure a legal basis for the processing of personal data under the Regulation;
- collect and transmit all personal data to the operator in a lawful manner;
- not issue instructions to the processor (operator) that would otherwise be in conflict with the Regulation or legal rights of data subjects;
- act as the contact point of data subject.

PROCESSING BENEFITS

Using the HelpCare system brings benefits to both the user and his / her clients and employees.

Benefit for	**Benefit Description**
user	ability to effectively deliver services to clients
user	opportunities to get new clients
user	demonstrate proper and continuous provision of services to clients
user	reduce the possibility of incorrect or poor quality service provision to clients
user´s employees	employee's assistance in carrying out the duties of the employment relationship
clients	better services from the user
clients	the client can prove, where necessary, that the service provided by the user was not up to standard

PROCESSING RISKS

As with any processing of personal data, the use of the HelpCare system also entails certain risks to the rights and freedoms of data subjects, particularly clients and employees. One of the key principles of the Regulation is a risk-based approach, which means that the controller (i.e. the user) has to

consider the risks to the rights and freedoms of individuals to assess the upcoming processing of personal data. This of course includes risks in the context of security measures. This can be illustrated on the principle of accuracy; the higher the risk arising from any inaccuracy of personal data processed, the greater the demands on the mechanisms for updating personal data.

"Risk" means a scenario describing a particular event (threat) and its consequences (damage) together with an estimate of its severity and likelihood. The Regulation imposes an obligation on the controller to take appropriate measures to ensure, and be able to demonstrate, compliance with the Regulation, considering, among other things, the potentially diverse and various risks to the rights and freedoms of individuals.

Threats to the rights and freedoms of data subjects in connection with the use of HelpCare system may, for example, be:

Threat	**Example of threat (for HelpCare)**	**Countermeasures of the operator**
Processing of inaccurate personal data	The system contains personal data that has not been updated	Contracts for the provision of HelpCare services shall include a provision that the user shall report any change to his or her personal data without delay to the operator.
Processing of personal data beyond the purpose	Personal data collected for the purpose of providing the service are subsequently used for the direct marketing of unrelated goods or passed on to a new recipient.	The operator processes the personal data of user's clients and staff only for the purpose of providing HelpCare services. The operator processes personal data of user's clients and staff only under a contract with the user that meets requirements concerning the processing of personal data.
Processing of personal data without legal basis	The system contains personal data of persons who have not concluded a contract with the operator or user	The operator´s internal policy stipulates that services can be provided only to persons who have entered into a contract with the operator or user.
Processing of personal data that was not expected by the data subject	Clients´ data is used for marketing purposes.	The Processing Agreement sets strict limits on the handling of personal data by the operator.

Loss of personal data	Damage of the data repository, leading to a lack of access to personal data.	A ban on transferring data from servers to local storage. Backup.
Theft of personal data	Hacker attack.	Depth Defense Strategy.
Abuse of access to personal data	The Administrator illegally copies the contact details of clients and hands them over to a third person for the purpose of offering goods or services.	Setting permission to access personal data. Contracts of confidentiality. Logging activities.

NAM System, a.s., as a personal data processor of the HelpCare system, carried out a risk assessment of the processing of personal data in the HelpCare system during the activities of the operator and the user and this assessment forms Appendix 1 of this policy.

NAM system, a.s., as a personal data processor of the HelpCare system, has adopted measures incorporated in this Policy to minimize the risk of loss or theft of personal data or misuse of access to parts of the HelpCare system under the processor´s control.

The controller (i.e. the user) is required to adopt effective measures against the risk of loss or theft of personal data or misuse of access to those parts of the HelpCare system under its control, in particular to procure the security and limitation of access to the computer equipment and mobile devices involved in the HelpCare system in order to prevent the unauthorized or unlawful destruction, loss, alteration or access to transferred, stored or otherwise processed personal data.

The administrator is also required to take effective measures against all other risks to the rights and freedoms of individuals with regard to the processing of personal data in the HelpCare system.

It is important to note that if the user intends to systematically monitor his/her employees or process clients' health data via the HelpCare system, the user is required to perform a so-called privacy impact assessment prior to commencement of these activities, and then perform the processing after the results of that assessment.

TECHNICAL AND ORGANIZATIONAL MEASURES TAKEN BY THE OPERATOR TO PROVIDE THE PROCESSING OF PERSONAL DATA IN ACCORDANCE WITH THE REQUIREMENTS OFTHE REGULATION AND PROTECTION OF PERSONAL DATA

Consideratng the state of technology, the costs of implementation and the nature, scope, context and purposes of processing as well as the various possibilities and severity of risk to the rights and freedoms of natural persons, the operator implemented technical and organizational measures to ensure the processing of personal data in accordance with the requirements of the Regulation and to ensure the protection of data subjects' rights:

1. The server of the HelpCare system is located in a secure technology center in accordance with current legislation. Only authorized employees of NAM System, a.s. who have signed a Non-Disclosure Agreement have physical access to the technology center. NAM system, a.s. is a holder of the National Security Authority certificate.

2. Technically, the operation of the technology center is ensured by multiple power supplies and an advanced defense system. An in-depth defense strategy ensures that security controls are present at different layers of service and if any area fails, there are compensatory controls that maintain security at all times. The strategy also includes tactics to detect, prevent and mitigate security breaches before they occur. This also includes continuous improvement of service security features, including:
   - Data encryption
   - Data Backup
   - Network traffic monitoring
   - Regular security updates
   - Risk detection and prevention at the network level
   - Multi-factor authentication to access services
   - Audit administrators´ access and activities
   - Continuous improvement of administrators´ competencies
3. Preventing violations of these rules also involves the controlled deletion of unnecessary accounts when the employee leaves the operator, changes work-group or does not use the account before it expires. Whenever possible, human intervention is replaced by an automated tool-based process, including routine functions such as deployment, debugging, diagnostics and restarting.
4. Checking Physical Access to the Technology Center uses multiple authentication and security processes, including smart cards, local security personnel, continuous video monitoring, and two-factor authentication. The technology center is monitored by motion sensors. In the case of natural disasters, security also includes automated fire and extinguishing systems.
5. User and client data are not passed on to any third party (for marketing, business offers, etc.) unless this has been imposed on the operator by a decision from a public authority and the system operator does not process the data in any way other than is necessary for provision of services.
6. NAM system, a.s. as a personal data processor, has adopted measures in the form of an internal policy to ensure that its employees (any natural person acting on behalf of the controller or processor) who have access to personal data process personal data in accordance with the rules set out in this policy and with the Regulation.
7. Subject to paragraph 8 below, the operator shall, after termination of the contract with the user, cease processing personal data on behalf of the user. Upon the user's written instruction, the operator shall also ensure (at the user´s cost) to return all personal data together with all the copies he owns or holds. If the user does not submit instructions to return data within two (2) months from the date of termination of the contract, the operator may erase all personal data, including copies thereof, unless the storage of personal data is required by law. If personal data shall be returned in accordance with the foregoing, they shall be returned in a usual, readable format that the parties have agreed on.
8. The operator may retain personal data only to the extent required by EU or national legislation and only for the period corresponding to the provisions of EU or national legislation and provided that the operator ensures the confidentiality of all personal data and that all personal data shall be processed only to the extent necessary for the purpose specified by EU or its member state legislation requiring their storage and not for any other purpose.
9. The operator has appointed a Data Protection Officer under Article 37 of the Regulation. Contact details of DPO are available at www.namsystem.cz/gdpr/.
10. The operator keeps records of all categories of processing activities carried out on behalf of the controller in accordance with Article 30, paragraph 2. of the Regulation.

Technical and organizational measures for processing of personal data adopted by the operator are described in more detail in Appendix 2 of this policy.

APPENDIXES:

1) Risk matrix – HelpCare
2) Technical and organizational measures for processing of personal data

Risk matrix - HELPCARE

		Unjustifiable collection or handling of personal data			Security breach			Aggregate
	Threat	Data inaccuracy Processing beyond purpose Processing without a legal basis Processing an unexpected by data subject			Loss of data Data theft Access violation			
Harm		**Likely**	**Severity**	**Score**	**Likely**	**Severity**	**Score**	**Risk rank**
Tangible harm								
Injury		0		0	0		0	**0**
The theft or misuse of identity		0		0	0		0	**0**
Financial loss		0		0	0		0	**0**
Significant economic disadvantage		0		0	0		0	**0**
Other material damage		0		0	0		0	**0**
Intangible harm								**0**
Violation of the protection of images of data subject		0		0	0		0	**0**
Invasion of privacy		0		0	3	5	15	**15**
Loss of control over personal data		3	3	9	1	4	4	**13**
Violation of letter secret		0		0	0		0	**0**
Harassment (spam)		0		0	0		0	**0**
Damage to the reputation		0		0	0		0	**0**
Psychological harm		2	1	2	0		0	**2**
Diskrimination		0		0	0		0	**0**
Excessive surveillance		3	3	9	0		0	**9**
Loss of confidentiality of personal data protected by professional secrecy		0		0	0		0	**0**
Unauthorized abolition of pseudonymization		0		0	0		0	**0**
Significant social disadvantage		0		0	0		0	**0**
Other intangible damage		0		0	0		0	**0**

Legend	**Aggregate risk rank**	**39**
Rank "Likely" from 0 (none) po 10 (surely)		
Rank "Severity" from 0 (none) po 10 (surely)		

TECHNICAL AND ORGANIZATIONAL MEASURES FOR PROCESSING OF PERSONAL DATA

1. ACCESS CONTROL TO PLACES WHERE PROCESSING OCCURS

The operator has implemented the following technical and organizational measures to prevent unauthorized persons from accessing places and facilities used for processing of personal data.
Technical and organizational measures to control access to these processing places may be as follows:

• Protective measures to prevent theft, manipulation and damage of data processing equipment;

• Security zones;

• Login of staff at the workplace;

• Controlled distribution of keys (including access areas);

• Physical security with 24/7/365 service;

• Safety documentation;

• Monitoring equipment, e.g. alarm system, camera surveillance system.

2. ACCESS CONTROL TO SERVER APPLICATION OF HELPCARE SYSTEM

The operator has implemented the following technical and organizational measures to prevent unauthorized persons access to personal data processed in the HelpCare server application. Unauthorized persons do not have access to the HelpCare server application.
The technical and organizational measures used to identify the user in the system may be as follows:
• Only authorized employees of the operator, who have entered into a Non-Disclosure Agreement, have physical access to the technology center;
• Access permission (passwords, codes, etc.);
• Security monitoring (administrator and user login);
• Automatic locking (e.g. password required for re-login);
• Process ensuring immediate revocation of all access rights if the employee terminates his/her employment process;
• Security backups;
• Antivirus protection;
• Encryption;
• Firewall;
• Continuously increasing the level of expertise of administrators;
• Safety documentation.

3. DATA ACCESS MANAGEMENT

The operator has ensured that persons authorized to use the HelpCare system have access only to the data to which they have access rights. Furthermore, the operator has ensured that this data could not be read, copied, altered or deleted by an unauthorized person in the HelpCare server application during processing, use, and other storage.
Measures for access and registration rights and their monitoring are as follows:

• Setting access permission according to specific needs (different levels of access to data);
• Data repositories are located in secure rooms that are regularly inspected for security;
• The principle of need to know (access to the minimum necessary information) is respected;
• Unknown / unauthorized software cannot be installed on the provider´s hardware;
• Data are kept encrypted;
• Safety documentation.

4. TRANSMISSION MANAGEMENT

The operator has implemented the following measures to ensure that during digital transmission, transportation or storage on data carriers, data may not be read, copied, altered or deleted.
Measures during transmission, transportation and storage of data on data carriers are as follows:
• Access measures (passwords, codes, etc.);
• Encryption;
• Coding, network connection (VPN = Virtual Network / virtual private network);
• Digital signature;
• User safety monitoring;
• Measures to prevent unmanaged data transmission (e.g. USB port locking);
• Safety documentation.

5. RECORDS MANAGEMENT

The operator has implemented the following measures to ensure that checks are made as to whether data was entered, modified or deleted in the processing system, and by whom.

Measures for the subsequent verification of whether the data were entered, modified or deleted, and by whom are the following:

• Security monitoring of users (read, change, unauthorized access attempts, etc., regular analysis of records / special analysis of records, if necessary);

• Regular evaluation of security monitoring;

• Safety documentation.

6. PROCESSING MANAGEMENT

The operator has implemented the following measures to ensure that personal data shall be processed only in accordance with the agreement concluded with the user.

Measures to differentiate obligations towards the user are as follows:

• Operator´s employees shall differentiate between the processing of data of the operator, user and other operator's clients (other users);

• The operator shall process the user´s data with at least the same care as the operator's own "confidential" data;

• The operator's internal policy shall ensure that its employees (any natural person acting on behalf of the controller or processor) who have access to personal data process such data in accordance with the rules set out in this policy and the Regulation;

• The operator has appointed a Data Protection Officer;

• Records of operators' processing activities.

7. DATA AVAILABILITY MANAGEMENT

The operator has introduced the following measures to ensure that personal data in the HelpCare system shall be protected against accidental destruction or loss.

Measures to prevent the destruction / loss of data are as follows:

- Backup;
- Separate storage;
- Disk mirroring (e.g. RAID);
- Multiple protection of power supplies;
- Regular checks of system status (monitoring);
- Antivirus protection;
- Emergency plan (including regular examinations);
- Automated fire and extinguishing systems
- Network traffic monitoring
- Regular security updates
- Risk detection and prevention at the network level

8. PROCESSING SEPARATION MANAGEMENT

The operator has implemented the following measures to ensure that the processing and storage of personal data collected for a particular purpose is done separately from any other data.

Measures to ensure separate processing of personal data (storage, alteration, deletion, transmission), if personal data were collected for different reasons, the operator adopts the following measures:

- Multi-client solution;

- Real-time separation of systems and environmental testing;

- Documented function separation;

- User and client data are not passed on to any third party (for marketing, business offers, etc.) unless this has been imposed on the operator by the decision of a public authority and the operator does not process data in any way other than necessary for the operation of services.