EU Data Information Notice	Information Notice Category	Date updated	Version
IntelligentCARE (ICM)	Connected product and related service(s) to a connected product].	28/04/2026	01

Manufacturer/Distributor	Service Provider
Access Techology A/S, CVR: 32831192	Access Techology A/S, CVR: 32831192
Geographical/physical address	**Geographical/physical address**
Marøgelhøj 22 C, 8520 Lystrup	**Marøgelhøj 22 C, 8520 Lystrup**

Data Information Notice

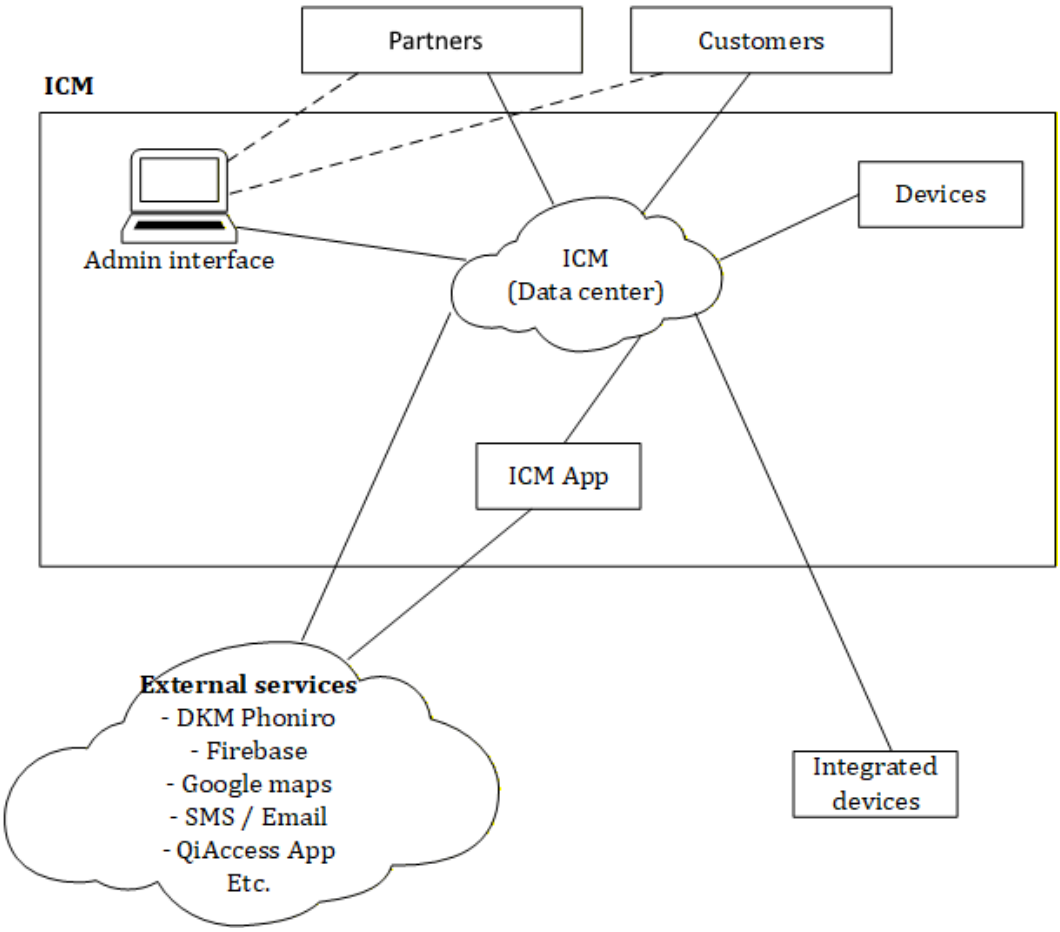
Introduction

General

This information notice explains how data generated by, or collected through, the IntelligentCare system (the "**Product**") is accessed, used, and shared (including to provide UI and API online interfaces, devices, gateways, apps, external and internal services and interfaces (the "**Service**")) and how the data is otherwise processed, in line with the requirements under Article 3 of the EU Data Act.

Product and service description

The Product constitutes an ecosystem of connected services, some hosted in a private cloud and others part being physical devices on site and again others are external services. The service is offered as B2B to municipalities, institutions and partners. The Product provides user and client management as well as alarm generation, reception and notification plus unlocking capabilities in the care domain (e.g. senior care, home care, psychiatry).



The Product, when deployed with a municipality or institution, generates technical and operational data, including but not limited to:

- Institution or municipality configuration
- Client (care receiver) configuration
- User (Care giver) configuration
- Device configuration
- Audit trail data for all access and modification of configurations
- Event data for all device activity, like messages, alarms, unlockings, location information, technical status alerts
- Technical information, like device firmware, app versions, battery status
- Trace data for notification and handling of alarms

Such data is transmitted to the Service in accordance with the technical capabilities of the Product and solely for the purposes of enabling the provision, maintenance, and security of the Service.

The Service processes this product data to facilitate core functionalities, including alarm generation, transmission and tracking, unlocking permission assignment, access control management, configuration oversight, and system level monitoring.

Data may be stored transitively on the devices or external services, but is stored according to the customers data retention policies inside the Product's hosted backend system. Service-related data, such as user provided personal information and access or audit logs required for the operation of The Product, is retained only for the duration necessary to fulfil the Service obligations or as otherwise determined by the customer's configuration.

Data holders

The following parties receive data from the Product and/or the Service and may use the data for their own purposes ('data holders'):

- Access Technology AS, Denmark
- EU Data Act 'User' of the service

Access Technology AS uses third-party service providers who process data on our behalf and on our instructions. These processors are not permitted to use the data for their own purposes. Our data processors include:

Name	**Product line**
Legrand Care	The Neat product line offering wrist transmitters, door sensors, emergency call devices etc. The products operate on both proprietary wireless communication and internet-based protocol SCAIP
Climax Technology	The Climax Telecare product line offering wrist transmitters, door sensors, emergency call devices, GPS trackers etc. The products operate on both proprietary wireless communication and internet-based protocol Cid and Sia-Cid.
MiniFinder	The MiniFinder GPS tracker product line offering different GPS trackers. The product operates on the internet-based protocol HTTP (REST based TLS)
Videx	The door phone product line. The product operates on the internet-based protocol HTTP (REST based TLS)
Aperio	The Aperio lock product line. The products operate on a ZigBee based proprietary protocol.
QiAccess	The Phoniro product line and QiAccess management and control system. The product operates on the internet-based protocol HTTP (REST based TLS)

Terms of use and quality of service

IntelligentCare is governed by Terms of Use, including SLA, and Privacy Statements provided to the customer upon purchase of the product and service

Data which the Product is capable of generating

Nature of data	Format	Estimated volume	Collection frequency	Data retention
Device data, which is any message generated by a device connected to the system, like a social alarm, a lock, a door operation or a motion detection.	Stored in SQL, exportable in JSON and CSV	>10MB an hour	Data is collected each time a device generates an observation, which may occur rarely or multiple times per minute	Data is stored transitively on devices until transferred to the server. Retention time set by customer, default to 5 months + 1 month recovery backup.
Audit trail data for all access and modification of configurations is generated on any configuration change or access request	Stored in SQL, exportable in JSON and CSV	<10MB a day	Data is collected each time a configuration is changed	Data is stored on the server Retention time is set by customer, default to 5 months + 1 month recovery backup.
Technical information, like device firmware, app versions, battery status	Stored in SQL, exportable in JSON and CSV	<10MB a day	Data is collected each time a device or App reports a technical update	Data is stored transitively on devices until transferred to the server. Retention time, after information becomes no longer needed, is set by customer, default to 5 months + 1 month

Nature of data	Format	Estimated volume	Collection frequency	Data retention
				recovery backup.
Trace data for notification and handling of alarms	Stored in SQL, exportable in JSON and CSV	>1MB an hour	Data is collected each time an alarm is forwarded to a care giver or when the alarm changes state	Retention time set by customer, default to 5 months + 1 month recovery backup.

Data obtained by The Product

Nature of data	Format	Estimated volume	Data retention
Configuration data, which is any data entered into the system regarding municipality/institution, users, clients and devices.	Stored in SQL, exportable in JSON and CSV	<10MB a day	Data is stored on the server (and for devices in their configuration). Retention time, after configuration becomes no longer needed, is set by customer, default to 5 months + 1 month recovery backup.

Data sharing and use

Type of data	Data use	Sharing of data	Identity of data recipient
Configuration data like personal information such as name, address, email etc. Device data, AuditTrail logs, Technical information and Trace data	The User has the possibility to access data.	Not shared with a third party.	The User have access to the data by access rights.

Data access and user capabilities

Direct access to data	Indirect access to data	Erasure of data
User can access all data provided by the user or generated by the Product based upon user access configuration - information such as client, user and device configuration, access and alarm logs, message logs, device status, technical information. The access to data is via API, online interface or export.	Product data in IntelligentCare backend can be retrieved by request to dataact.seniorcare@assaabloy.com	The User can delete all configuration data using the online interface or via API. Data generated by the Product is subject to the Data Retention time, which is also controlled by the User.

How to request data sharing

You may request us to share data with a specific third party by by e-mail: dataact.seniorcare@assaabloy.com. We may under certain circumstances deny a request of data sharing to third parties.

You can withdraw your request for data sharing at any time by by e-mail: dataact.seniorcare@assaabloy.com. Once withdrawn, we will cease transferring data.

Right to lodge a complaint

If you believe our handling of your data infringes your rights under applicable legislation, you have the right to lodge a complaint with the competent authority in your jurisdiction.

Trade secrets

In some cases, data from the connected products or related services may include trade secrets that we or our partners own. Trade secrets shall be preserved and disclosed only where all necessary measures prior to preserve their confidentiality are taken, in particular regarding third parties. In exceptional circumstances, our ability to grant access to data may be limited due to trade secrets.

We maintain confidentiality obligations to protect any trade secrets contained within your data.

Term and termination

Your contract with IntelligentCare is valid as of the effective date of the relevant agreement, beginning on the date you sign up or otherwise agree to the Terms of Use of the Service.

You may end the contract by contacting your sales representative and requesting termination. Specific conditions and notice periods may apply as specified in your contract.

Contact information

Should you have any questions regarding the data generated by the Product or the Service, do not hesitate to contact us at dataact.seniorcare@assaabloy.com.