Data Act notice

Effective from: 12.09.2025
Last update: 27.10.2025
Version: 1.1
Data classification: Public information

Purpose and legal basis

Safe4 Security Group AS, including its subsidiaries (collectively referred to as "Safe4 Security Group", "Safe4", "we", "us", or "our"), provides this notice to explain how data generated by connected products and related services is made available to customers in the European Union and other applicable markets where the EU Data Act applies. This notice applies to all services operated on the Safe4 platform, including Iotiliti, HomeSecurity, Confi.care, and partner-branded solutions. The policy ensures transparency and compliance with regulatory requirements for access, sharing and portability of product- and service-generated data.

Service delivery and platform context

Safe4 operates a unified platform with a gateway, connected sensors, and mobile applications, all integrated with a cloud-based IoT platform. The platform is designed for secure, reliable operation and is regularly updated to meet regulatory and industry requirements. Service modules differ by use case, but share the same technical foundation and operational controls across brands and partner channels.

Roles and responsibilities

Under the Data Act, the user is the natural or legal person using the connected product and related service. Safe4 is the data holder for user data generated by platform operation and is responsible for making this data available in accordance with regulatory obligations. Where a manufacturer or distributor (such as a white-label partner) is also a data holder, the user submits the request to that party. Safe4 coordinates with the partner and supplies the relevant platform user data for fulfilment, ensuring the user does not need to manage multiple parallel requests.

Data types, use and format

User data includes device and sensor status and activity, device types and identifiers, log and event histories, connection quality, firmware version, alarm and access events, automation outcomes, system configuration, activity logs, system messages and user-defined metadata (e.i. room names, device groups, modes). User data is used to deliver service functionality, notifications and alarms, maintain reliability, and enable continuous platform improvement.

Data is provided as a CSV file by default. Documentation of field structure and metadata is included with each export. Other formats may be considered for special cases if technically feasible and agreed in advance. Personal data (names, addresses, phone numbers, emails) is not included in Data Act exports unless lawfully required. Mixed datasets are processed in accordance with GDPR and our Privacy Policy.

Access, frequency and delivery to a third party

Users and authorized third parties have the right to access and receive user data without undue delay. Standard requests are typically processed within 30 days. Delays may occur due to technical complexity, verification requirements, or maintenance. Access can be requested by contacting compliance@safe4.com from the registered account email. All requests are subject to authentication, scope, and frequency controls, and may be refused if they threaten security, confidentiality, or trade secrets.

For third parties, Safe4 supports both one-time exports and, by specific agreement, ongoing access via dedicated API. API access is available only upon request and subject to a separate agreement, including compensation for onboarding, setup, and direct costs.

Restrictions and limitations

Access may be restricted for the following reasons:

- The request is excessive, abusive or threatens platform stability (“fair use” means a reasonable frequency and volume based on normal usage).
- The data requested contains confidential know-how or trade secrets beyond the scope of Data Act obligations (e.g. internal diagnostics, proprietary algorithms, security architecture).
- Technical feasibility: Safe4 may limit format, delivery method, or frequency if the platform cannot support continuous or high-volume access without risk.

Storage, security and retention

All user data is processed and stored in the EU in secure, professionally managed infrastructure. Encryption is applied in transit and at rest. Access is governed by role-based controls, audit logging, and regular review. Configuration and account-linked data are retained while the account or installation is active. Operational events and diagnostics are deleted or anonymized on a rolling basis. Upon termination, user data is deleted according to legal retention requirements and Safe4’s internal policy.

Portability and change of provider

Any user or business customer may request a structured export of user data to support a change of provider. Safe4 will facilitate coordinated handover, in a commonly used, machine-readable format, and provide metadata and field documentation to enable interoperability.

Updates and contact

This notice is versioned and updated to reflect regulatory or service changes. The current version is published on the Safe4 website.

Version history

Version	Date	Description	Author	Approver
1.1	27.10.2025	Update	August Brekkhus	Sjur Jensen Bay
1.0	12.09.2025	Initial release	August Brekkhus	Sjur Jensen Bay