Privacy Policy

Policy Owner: Marcus Agdestein
Effective Date: 05.10.2026
Data Classification: Public

1. Introduction

This Privacy Policy explains how Safe4 Security Group AS, including its subsidiaries (collectively referred to as "Safe4 Security Group AS", "Safe4", "We" or "the Company"), collects, uses, shares and protects personal data when you use or interact with our websites, applications, platforms, products and services.

We process personal data in accordance with applicable data protection laws, including the General Data Protection Regulation (GDPR).

2. Data controller

Responsible entity
Safe4 Security Group AS
Maridalsveien 300, 0872 Oslo, Norway

Data Protection Officer
Our Data Protection Officer is responsible for overseeing our GDPR compliance program and can be contacted for any data protection inquiries:
Marcus Agdestein (CFO)
mag@safe4.com
+47 959 39 167

3. Personal data we collect

The personal data we collect depends on how you interact with Safe4 and which services you use. This may include:

- **Contact and account information**, such as name, email address, phone number, address and account details.
- **Order and payment information**, such as billing and delivery information, payment details and order history.
- **Technical and usage data**, such as IP address, device information, browser information, log data and information about how our websites, applications and services are used.
- **Service and device data**, including information related to connected devices, installations, alarm events, service requests, images or video recordings where camera services are used, and other data generated through our platforms and services.
- **Communication data**, such as messages submitted through contact forms, support requests and telephone recordings where applicable.

- **Marketing data**, such as newsletter interactions, website activity and preferences where marketing or analytics tools are used.

We may also receive personal data from customers, partners, service providers, integrations, public registers or other third parties where relevant to providing our services or meeting legal obligations. Where we process special categories of personal data, this will only be done where permitted by applicable law and where appropriate safeguards are in place.

4. Purposes and legal basis for processing

We process personal data for specific purposes and only where we have a valid legal basis under Article 6 of the General Data Protection Regulation (GDPR).

4.1 General purposes for processing

Purpose	Legal basis	Examples
Customer Service	Performance of a contract (Art. 6(1)(b)) or Legitimate interests (Art. 6(1)(f))	Responding to inquiries and providing customer support, including the use of automated tools and artificial intelligence to assist with support activities.
Order and Subscription Processing	Performance of a contract (Art. 6(1)(b))	Processing orders, payments, deliveries and subscriptions.
Contract Fulfillment	Performance of a contract (Art. 6(1)(b))	Providing, operating and supporting our products and services for customers and partners.
Compliance with Legal Obligations	Legal obligation (Art. 6(1)(c))	Processing or retaining information where required by applicable law or regulation.

4.2 Emergency response

In emergency situations, such as triggered alarms, we may process personal data where necessary to protect your vital interests or those of another individual, for example by identifying the person concerned or notifying emergency contacts or authorities.

Purpose	Legal basis	Examples
Emergency response	Vital interests (Art. 6(1)(d))	Identifying the person concerned or notifying emergency contacts or authorities during alarm events or other emergencies.

4.3 Analytics and service improvement

We may process personal data to analyze, maintain and improve our websites, applications, products and services, including to improve functionality, performance and user experience. This may include analyzing service, usage and sensor data where relevant.

Purpose	Legal basis (GDPR Art. 6)	Examples
Analytics and statistics	Legitimate interests (Art. 6(1)(f)) or Consent (Art. 6(1)(a))	Understanding how our websites, applications and services are used and improving their performance.
Service improvement	Legitimate interests (Art. 6(1)(f))	Analyzing service, usage and sensor data to improve functionality, reliability and user experience.

4.4 Marketing and Profiling

We may process personal data for marketing and profiling purposes based on your consent or, where permitted, our legitimate interests.

You may withdraw your consent at any time. Where cookies or similar technologies are used for marketing or analytics, you can manage your preferences through the cookie settings available on our websites

Purpose	Legal basis (GDPR Art. 6)	Examples
Marketing	Consent (Art. 6(1)(a)) or Legitimate interests (Art. 6(1)(f)) where permitted	Sending newsletters, offers or other relevant communications.
Profiling	Consent (Art. 6(1)(a))	Using website and communication activity to understand interests and improve the relevance of marketing.

5. Sharing of personal Data

We may share personal data with the following categories of recipients where necessary:

- **Analytics providers:** For website analytics and service improvement.
- **Marketing providers:** For newsletters, advertising and marketing activities.
- **Payment providers:** For processing payments, orders and subscriptions.
- **IT service providers:** For hosting, development, infrastructure and technical support.
- **Administrative providers:** For accounting, invoicing and other administrative services.
- **Operational service providers:** For delivering and supporting our services, including alarm response and related services.
- **Logistics providers:** For delivery of hardware and orders.
- **Partners and distributors:** Where necessary to provide products or services.
- **Authorities:** Where required by law or where necessary to protect legal rights or safety.

Personal data may also be shared between Safe4 Security Group AS and its subsidiaries where necessary for administrative, operational or service-related purposes.

Where third parties process personal data on our behalf, appropriate contractual and data protection requirements are applied in accordance with applicable law. Third parties are provided access only where necessary for the services they provide. An up-to-date overview of relevant service providers and subprocessors is available through our Trust Center at https://trust.safe4.com.

6. Data retention

We retain personal data only for as long as necessary for the purposes for which it was collected, or as required by applicable law, regulation or contractual requirements.

6.1 General retention periods

We retain your personal data only as long as necessary for the purposes outlined or as required by law:

Data type	Retention period
Invoicing and order data	5 years, as required by the Norwegian Accounting Act
Marketing and analytics data	Retained only as long as necessary for the relevant purpose or until consent is withdrawn, where processing is based on consent
General communications and correspondence	5 years
Support requests and related communication	3 years

6.2 Service-specific retention periods

Some of our services process data through the Safe4 IoT platform and our Alarm Receiving Centre (ARC) systems. The IoT platform supports connected devices and related service functionality, while the ARC systems are used for alarm monitoring and response.

Safe4's Alarm Receiving Centre is certified according to EN 50518, a strict European standard for alarm receiving centres. The standard requires certain operational and alarm-related data to be retained for three years.

Data type	Context	Retention period
Alarm and device activity logs	IoT platform	30 days after the event occurs
User change history	IoT platform	1 year
Location data and usage logs	IoT platform	Until termination of the customer relationship
User data	IoT platform	3 months after termination of the customer relationship
Camera recordings	IoT platform	7 days
Camera snapshots sent to the Alarm Receiving Centre	ARC software	7 days
Gateway data	ARC software	Until termination of the customer relationship

User and customer data	ARC software	3 years after termination of the customer relationship, plus up to 3 months
Logs	ARC software	3 years after termination of the customer relationship, plus up to 3 months
Telephone recordings	ARC telephony system	3 months

7. Data security

We implement appropriate technical and organizational measures to protect personal data against unauthorized access, loss, misuse, alteration or disclosure. These measures include access controls, encryption, secure development practices, monitoring and other security controls appropriate to the nature and sensitivity of the data.

Safe4 maintains an information security management system certified to ISO 27001 and regularly assesses security risks and controls. More information about our certifications and security practices is available through our Trust Center at https://trust.safe4.com.

In the event of a personal data breach, we will assess the incident and notify affected individuals, customers and relevant supervisory authorities where required by applicable data protection law.

8. Your rights

Under GDPR, you have the following rights regarding your personal data:

- **Access:** Request a copy of your personal data.
- **Rectification:** Request correction of inaccurate personal data.
- **Erasure:** Request deletion of your personal data, subject to applicable legal requirements.
- **Restriction:** Request that we limit the processing of your personal data.
- **Objection:** Object to certain processing based on legitimate interests.
- **Data portability:** Receive certain personal data in a structured, commonly used and machine-readable format.
- **Withdraw consent:** Withdraw your consent at any time where processing is based on consent.
- **Lodge a complaint:** Contact the Norwegian Data Protection Authority (Datatilsynet).

To exercise your rights, please contact us at compliance@safe4.com. We will respond in accordance with the time limits required under applicable data protection law.

9. International data transfers

Where personal data is transferred outside the EU/EEA, we ensure that appropriate safeguards are in place in accordance with applicable data protection law. This may include adequacy decisions, Standard Contractual Clauses (SCCs), or other approved transfer mechanisms.

10. Changes to this policy

We may update this Privacy Policy from time to time. The latest version will be made available through our websites and services. Where required by law, we will provide appropriate notice of material changes.

Version history

Version	Date	Description	Author	Approver
2.1	05.10.2026	Revision and update	August Brekkhus	Sjur Jensen Bay
2.0	27.03.2025	New structure	August Brekkhus	Sjur Jensen Bay
1.1	07.10.2025	Minor adjustments	Asbjørn Aasen	Asbjørn Aasen
1.0	15.10.2023	New structure	Asbjørn Aasen	Asbjørn Aasen