Privacy Policy

Policy Owner: Marcus Agdestein
Effective Date: Mar 24, 2025
Data classification: Public Information

Introduction

This Privacy Policy outlines how Safe4 Security Group AS, including its subsidiaries (collectively referred to as "Safe4 Security Group", "Safe4", "we", "us", or "our"), collects, uses, and protects personal data when you interact with our websites (e.g., safe4.com, onestiproducts.io, iotiliti.com, confi.care, safeunlock.no, safe4risk.com), our IoT platform, our Alarm Receiving Centre (ARC) software, or any other services we provide. We are committed to safeguarding your privacy in accordance with the EU General Data Protection Regulation (GDPR) and Norwegian data protection laws.

By accessing or using our websites, platforms, or services, you consent to the processing of your personal data as described in this policy. If you do not agree, please refrain from using our services.

At Safe4, we take data protection seriously and leverage GDPR compliance tools and have conducted a Data Protection Impact Assessment (DPIA) for large-scale data collection via our IoT platform, as recommended by the Norwegian Data Protection Authority (Datatilsynet). We have implemented comprehensive GDPR policies, including technical, physical, and administrative safeguards, to ensure compliance and safeguard your data.

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

Personal Data We Collect

We collect the following personal data depending on how you interact with us:

- **Across All Websites:**
  - Technical data: IP address, browser details, device information, and pages visited (via server logs and analytics tools).
  - Cookies: See our Cookie Policy, available in the footer of our websites and/or as a pop-up.

- **Via Contact Forms:** Name, email address, phone number (if provided), and message content.
- **For Websites with Orders, Subscriptions, or Online Store:** Name, email address, phone number, billing address, delivery address, payment information, and order history.
- **Via IoT Platform:** Name, email address, phone number, installation address, and technical data from connected devices (if applicable).
- **Via Alarm Receiving Centre (ARC) Software:** Name, phone number, installation address, and data related to alarm events or service requests.
- **Marketing and Profiling:** Name, email address, behavioral data (e.g., website visits, clicks on newsletters) linked to your identity when you submit a form

We do not process sensitive personal data, such as health data, unless explicitly required and with your consent.

Purposes and Legal Basis for Processing

We process personal data for the following purposes and based on the legal bases outlined in GDPR Article 6:

Purpose	Legal Basis (GDPR Art. 6)	Examples
Customer Service	Contract (Art. 6(1)(b)) or Legitimate Interest (Art. 6(1)(f))	Responding to inquiries via forms or email.
Order/Subscription Management	Contract (Art. 6(1)(b))	Delivering products/services and fulfilling purchase agreements.
Contract Fulfillment	Contract (Art. 6(1)(b))	Supporting partners/customers via IoT platform or ARC software.
Legal Obligations	Legal Obligation (Art. 6(1)(c))	Retaining invoicing/order data for 5 years per Norwegian Accounting Act.
Analytics and Statistics	Legitimate Interest (Art. 6(1)(f)) or Consent (Art. 6(1)(a))	Improving websites/services via anonymized data or consent-based tools.
Marketing	Consent (Art. 6(1)(a)) or Legitimate Interest (Art. 6(1)(f))	Sending newsletters or offers (opt-out available for existing customers).
Profiling and Cross-Site Insights	Consent (Art. 6(1)(a))	Linking behavioral data across websites to understand user preferences.

Profiling and Cross-Site Data Collection

We use tools like HubSpot to analyze your interactions across our websites (e.g., visit history) and link this data to your identity (e.g., name, email) when you submit a form. This allows us to better understand your preferences and tailor our services or marketing efforts. Such profiling and cross-site data collection occur only with your explicit consent (via cookie consent tools or other opt-in mechanisms). You may withdraw consent at any time without affecting the lawfulness of prior processing.

The only automated decision-making we perform is sending automated emails (e.g., newsletters or follow-ups) based on your preferences, which you can opt out of at any time.

Sharing of Personal Data

We share your personal data with the following categories of recipients:

- **Analytics Tools:** For website and service improvement (e.g., Google Analytics).
- **Marketing Platforms:** For newsletters and targeted advertising (e.g., HubSpot, Facebook).
- **Payment Providers:** For processing orders and subscriptions.
- **IT Service Providers:** For hosting, development, and technical support (e.g., Microsoft, AWS).
- **Administrative Providers:** For accounting, invoicing, and financial management (e.g., accounting systems and accountants).
- **Service Providers:** For operational support (e.g., security guards responding to alarms via ARC software).
- **Partners and Distributors:** To fulfill contracts or deliver services on our behalf.
- **Authorities:** When required by law.

Data shared internally between Safe4 Security Group AS and its subsidiaries is processed under our legitimate interest for administrative purposes. All third parties processing personal data on our behalf are bound by Data Processing Agreements (DPAs) in accordance with GDPR.

Data Retention

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

- Invoicing and order data: 5 years, as required by the Norwegian Accounting Act.
- Behavioral data from profiling: Deleted upon withdrawal of consent or after 3 years of inactivity.
- Other data: Retained for 5 years unless otherwise specified.

Retention periods are determined based on legal requirements and best practices.

Data Security

We implement robust technical and organizational measures, including strong cryptography for data storage and transmission, as outlined in our Secure Development Policy, which incorporates privacy and security by design principles. In relation to ISO 27001 certification, we conduct regular security audits and risk assessments to protect your data from loss, misuse, or unauthorized access.

In the event of a personal data breach, Safe4 will notify affected data subjects, supervisory authorities (e.g., the Norwegian Data Protection Authority), and relevant customers (where Safe4 acts as a data processor) without undue delay, in accordance with GDPR requirements and our GDPR Breach Procedures and Incident Response Plan. We document all breaches, their effects, and remedial actions taken, unless the breach is unlikely to result in a risk to your rights and freedoms or is protected by technical measures such as encryption.

Your Rights

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

- **Access:** Request a copy of your data.
- **Rectification:** Correct inaccurate data.
- **Erasure:** Request deletion of your data (subject to legal retention obligations).
- **Restriction:** Limit processing of your data.
- **Objection:** Object to processing based on legitimate interest (e.g., marketing).

- **Data Portability:** Receive your data in a structured, machine-readable format.
- **Withdraw Consent:** Revoke consent at any time via cookie consent tools or by unsubscribing using the link in our emails
- **Lodge a Complaint:** Contact the Norwegian Data Protection Authority (Datatilsynet) at www.datatilsynet.no.

To exercise your rights, please email us at personvern@safe4.com. We will respond within one month, as required by GDPR.

International Data Transfers

We do not transfer personal data outside the EU/EEA unless strictly necessary and in full compliance with the safeguards required under the General Data Protection Regulation (GDPR). Where such transfers occur, they are conducted in accordance with appropriate legal mechanisms, such as the European Commission's Standard Contractual Clauses (SCCs), to ensure an adequate level of data protection. For instance, data processed by IT service providers, including but not limited to Microsoft and AWS, may be transferred to the United States. In such cases, these transfers are governed by Data Processing Agreements (DPAs) and SCCs to guarantee compliance with GDPR and ensure that data subjects' rights and freedoms are adequately protected.

Changes to This Policy

We may update this Privacy Policy from time to time. Significant changes will take effect 30 days after posting on our websites. Users who receive newsletters will be notified via email, and all affected users will be informed by email where required.

Version history

Version	Date	Description	Author	Approver
1.0	Oct 15, 2023	New structure	Asbjørn Aasen	Asbjørn Aasen
1.1	Oct 07, 2024	Minor adjustments	Asbjørn Aasen	Asbjørn Aasen
2.0	Mar 24, 2025	New structure	August Brekkhus	Sjur Jensen Bay