creditsafe

GDPR Customer Briefing

How Creditsafe is using GDPR to drive better business

Introduction

This document provides information about how the GDPR and Data Protection Act 2018 applies to Creditsafe's products and services. For further information about how Creditsafe uses data, readers should refer to the Privacy Notice and Transparency Statements, which can be found at the foot of Creditsafe's website.

Creditsafe Information Services.

Creditsafe operates in a business to business (B2B) environment and collects data on businesses from a variety of sources, both publicly available registries and from partner companies. The data Creditsafe collects is used in a variety of products and services. Personally Identifiable information (PII) which is handled by Creditsafe is only of those individuals who are directly connected to a business entity such as a director, or as a sole trader where the individual is the business.

The exception to the above is Creditsafe's businesses in Sweden and Norway where it also collects and processes data on consumers under the provisions of credit reference laws.

Lawful Basis to Deliver Information Services

Creditsafe processes data under two lawful bases; Legitimate Interests and Contract.

GDPR Article 6b permits the processing of personal data for the performance of a contract, or in order to take steps at the request of the data subject prior to entering into a contract. When Creditsafe provides products and services to its customers, the lawful basis will be under Contract.

GDPR Article 6f permits the processing of personal data for the purposes of the legitimate interests pursued by the data controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

The legitimate interest that Creditsafe operates under is that we are facilitating businesses to make risk based financial decisions in order to enable our clients to make better business and economic decisions. As such we also maintain the legitimate interest to make businesses aware of this capability.

Controller to Controller relationship

In the main the relationship between Creditsafe and its customers is a Controller to Controller relationship. This is because Creditsafe determines the purposes and means for collecting and processing the data and therefore is wholly responsible for all of its processing activities and must ensure that it only shares personal data when it is lawful to do so. Creditsafe's customers are also data controllers because they determine the purposes for processing the information that it has received, e.g. how to use the reports or prospecting lists, and is also responsible for ensuring that it processes this data lawfully.

Contractual terms can be found in Creditsafe's Terms & Conditions, including information about reasons for lawfully using Creditsafe's products, and more information about the processing can be found in the Transparency Statements on Creditsafe's website, depending on the products and services being provided.

Can our customers use our information?

Yes. However the Customer is responsible for establishing the lawful basis for processing personal data obtained pursuant to use of the information services of Creditsafe and maintaining compliance with the

Data Protection Legislation in connection with such data. And the Customer must also acknowledge that accessing personal data through the use of the information services of Creditsafe is only permitted where the customer has a lawful basis for doing so.

This means, for instance, that the customer shall only use the Creditsafe information services for the purpose of credit checking, prospecting, direct marketing, know your customer checks, compliance, data verification and enhancement, other lawful business due diligence purposes or all other business to business purposes with a legitimate interest with respect to the GDPR.

How Creditsafe has aligned with GDPR

Creditsafe has taken a total business approach to GDPR and reviewed all business processes and data process to ensure that they align with the legitimate interests of our business to support its customers to make financial decisions based on factual risk assessments. This process has allowed us to examine the sources and use of all of our data in order to ensure we can provide our customers with the services they want, while ensuring that none of our practices will cause harm or detriment to and individuals identified within our data sets.

Understanding our data sources and uses (data mapping)

For all stages of data custody we look to identify where we collect data from, what we are doing with data, how we are protecting data and how we are ensuring we do not infringe on the rights of the subject of that data, see the Privacy Policy and Transparency Statements for more details. This includes that personal data shall be obtained only for specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Lawful bases for processing

Creditsafe has systematically assessed each processing activity for its lawful basis. In the main it relies on Legitimate Interests for collecting data and marketing its services to other businesses and Contract for supplying products and services to its customers

Protecting the rights of the individual

Creditsafe has processes in place to address all the rights of individuals including Subject Access Requests (SAR), Right to Erasure, Right of Rectification, Rights to Data Portability, Right to Object to Processing and Right to Restrict Processing. However it should be noted that where information is gathered from public registries it may not be possible for Creditsafe to rectify or erasure information about a company, its directors or shareholders.

Data integrity

Creditsafe's Data Vault processes manages and stamps the data, which will ensure full traceability of all Creditsafe data. By clearly showing where the data has come from and any changes made with the reason for the change means that the integrity and quality of the data is enhanced.

Implementing appropriate technical and organisational measures to protect data

Creditsafe implements technologies which will allow us to protect against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Creditsafe is ISO27001 accredited. Examples of the technical measure implemented are as follows:

- Firewalls – All network ingress/egress points are protected by firewalls.
- DMZs – Well-defined for public-facing servers, with internal network segmentation used to further isolate sensitive resources.
- HIDS/NIDS – Enabled at key choke points on the network.
- SIEM – Logs generated by applications and infrastructure are fed into and monitored by a SIEM

system, with security events logged and analyzed with automated alerts in place.

- Anti-virus/anti-malware – All compatible endpoints covered by endpoint security software, with automatic updates.
- File Auditing - We use an Industry-leading data auditing solution for monitoring access and changes made to files containing personal data.
- Network/Host Scanning – Regular scanning and remediation for vulnerable configurations.
- Regular penetration testing, web application testing and vulnerability scanning – Threat and vulnerability management programme in place to remediate vulnerabilities.
- Data Loss Prevention: Creditsafe are currently implementing controls to detect and restrict unauthorized data movement while in motion, and at rest.

Additionally Creditsafe has comprehensive organizational measures, including a set of policies and procedures and regular training on data protection and information security, to ensure compliance with the regulations.

These technical and organizational measures combine to ensure that the data is not misused or removed outside of the Creditsafe infrastructure through unauthorized actions.

International Transfers

Creditsafe ensures that it will not transfer data outside the EEA unless it is to a country that has been deemed by the EU to have adequate data protection laws, or where there are suitable contracts in place to allow the transfer of data.

Being ready to respond

Creditsafe have implemented processes which will allow a quick and efficient response to any suspected incident, including any breaches that could impact PII data. Creditsafe are ready with clear and concise communication plans to clients, data subjects and regulatory authorities in the case of an incident which will result in any individual affected.

Privacy by Design

Creditsafe realizes that GDPR is not a single event in history. Instead it is being used as a guideline for our future business models with privacy by design being adopted in our interactions with individuals and in our business strategy ensuring all future business decisions and developments consider the impact on the individual before we go forward.

FAQ’s

Are Creditsafe fully GDPR compliant?

Creditsafe have a programme of continuous improvement and audit to ensure that its operations and services are in full alignment with the regulation.

Is Creditsafe regulated?

Yes. Creditsafe is regulated by the FCA and registered as a data controller with the UK Information Commissioner’s Office.

What security software and encryptions do you have in place to protect all data that Creditsafe have collected and/or processed?

- Creditsafe are ISO27001 certified.
- Creditsafe operates through a Tier3+ UK data centre, which is audited to ISO9001, ISO14001, ISO27001, ISAE3402, SSAE16 and PCI DSS standards.
- Comprehensive data centre physical security, including a 6-layer wall design, 24/7 campus patrols, military grade fencing, digital tripwires, multiple IR CCTV towers and is constructed to Californian earthquake standards.
- Creditsafe security controls include:
    - Firewalls – All network ingress/egress points are protected by a firewall.
    - DMZs – Well-defined for public-facing servers, with internal network segmentation used to further isolate sensitive resources.
    - HIDS/NIDS – Enabled at key choke points on the network.
    - SIEM – Networks monitored by SIEM, with security events logged and analysed, and automated alerts and alarms in place.
    - Antivirus – All compatible endpoints covered by anti-virus software, with automatic updates via an update server and the Internet.
    - Data Encryption
    - Network/Host Scanning – Regular scanning for vulnerable configurations.
    - Regular penetration testing, web application testing and vulnerability scanning – Threat and vulnerability management programme in place to manage output.
    - Data Backup - Data is replicated at 5 minute intervals from the Creditsafe production environment to a dedicated business continuity environment. The platform is sized and configured to use high availability, allowing automated fail-over of servers.

Where is all the data stored?

All Creditsafe data is stored either within the UK or within the EEA on secure servers which are fully protected for disaster recovery.

Creditsafe Marketing Data

Lawful bases.

Creditsafe ensures that all data is collected and used under proper permission, be that consent or legitimate interest.

For the compilation of prospecting lists for its customers, Creditsafe processes the data under Legitimate Interests. For the sale of these lists the lawful basis is Contract.

For marketing Creditsafe's products to its client the lawful basis is Legitimate Interest. Customers may opt out of marketing messages at any time.

Usage of data is fully mapped throughout the business and subjected to rigorous risk and data protection impact assessments as well as Legitimate Interest Assessments where appropriate.

What consent do Creditsafe ask from the businesses?

Consent obtained by Creditsafe is relevant to the use of the data being collected at that point, i.e. consent for use, marketing consent, consent for calling and consent for updating records for future contact.

In circumstances where consent is not available, GDPR Article 6f permits the processing for the purposes of the legitimate interests pursued by the controller or by a third party. The legitimate interest that Creditsafe operates under is that we are facilitating businesses to make risk based financial decisions in order to enable our clients to make better business and economic decisions. As such we also maintain the legitimate interest to make businesses aware of this capability, including when they are in the pursuit of new business opportunities.