creditsafe

GDPR Customer Briefing

How Creditsafe is using GDPR to drive better business

creditsafe

Introduction

What is GDPR?

The GDPR (General Data Protection Regulation) will provide a robust set of rules for the collection, storage and processing of personal information and comes into force on May 25th 2018. The GDPR is a regulation rather than a directive, which means it is a single piece of legislation that applies across all EU member states. As the UK will still be a member of the EU in 2018 it therefore applies to the UK in the same way, and will also apply after Brexit. Following the UK's exit of the EU, UK data protection laws are expected to align closely with all GDPR requirements with only minor derogations, meaning compliance with GDPR is not only necessary come the 25th May, but also likely to provide a benchmark for a future regulation.

Why GDPR?

With businesses gathering vast amounts of personal data on consumers from behavioural analytics to personal characteristics, the subject of personal privacy and protection has become a major concern. Many companies have developed extensive business models that are driven by trading information in exchange for access to services. While this offers tremendous opportunities, it also gives individuals little control over what their data is used for, how it is stored and by consequence, could leave them at threat to theft, fraud and other missuses. By strengthening measures, the EU strives to improve trust and reduce the overall threat to individuals.

The GDPR is introduced to reflect the advancement in technology and data over the past two decades. The GDPR aims to harmonise data privacy laws across Europe, creating an equal playing field and more importantly, making it simpler for businesses to understand and manage their own compliance.

Who does GDPR apply to?

All organisations that hold personal data on EU citizens will be affected by GDPR. It doesn't matter where the data is located in the world.

GDPR widens the *definition of personal data* to encompass anything that can be used to directly or indirectly identify a person. This covers a broad spectrum of data from names, photos, email addresses, bank details and posts on social networking sites to medical information or IP addresses, as an example. The new regulation seeks to protect this data, whether its filing is automatic or manual, paper or electronic.

When considering B2B vs B2C data, and what does or does not fall under the remit of GDPR, the line separating personal and business data seems not always a clearly defined one. For example, data of individuals from unincorporated businesses such as Sole Traders or Partnerships, or director-data of incorporated businesses should be considered as personal identifiable data under the definition of GDPR.

creditsafe

Who are the key actors in GDPR?

Organisations will be accountable to the data protection supervisory authorities. Whilst the accountability is not a new requirement, GDPR requires all organisations to record and document compliance with all applicable aspects of GDPR. The regulation gives individuals more rights in respect of their data, including more control and visibility of how their personal data is being used, and the right to have that information removed or moved if requested.

Data-subject

Data-subjects are the private individual persons (EU citizens) on which data is collected and processed, for instance directors, shareholders and business owners. GDPR provides data-subjects with more rights with regards to the data that is being processed and controlled by businesses. This is usually referred to as *empowerment* of the data-subjects.

Data-controller

The data-controller determines the purposes and means of processing personal data. They will control the manner in which personal data is processed, meaning they have ownership over the "why" and "how" of all data processing. Data-controllers are not relieved of their obligations where a processor is involved – the GDPR places further obligations to ensure your contracts with processors comply with the GDPR. Creditsafe is a data-controller.

Data-processor

The data-processor is responsible for processing personal data on behalf of a controller. The GDPR places specific legal obligations on data-processors; for example, they are required to maintain records of personal data and processing activities. Data-processors will have legal liability if they are responsible for a breach.

Data Protection Authority (DPA)

DPAs are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law. They provide expert advice on data protection issues and handle complaints lodged against violations of the General Data Protection Regulation and the relevant national laws. There is one in each EU Member State.

Data Protection Officer

The primary role of the Data Protection Officer (DPO) is to ensure that the organisation processes the personal data of its staff, customers, providers or any other individuals in compliance with the applicable data protection rules. In the EU institutions and bodies, the applicable Data Protection Regulation (Regulation (EC) 45/2001) obliges them each to appoint a DPO. Creditsafe has appointed a DPO at Group level and has local staff supporting the DPO role where regulation or business practice deem necessary.

creditsafe

The Key Areas of GDPR

1. **Accountability**

   Data-controllers must be able to demonstrate the organization's compliance with the GDPR. However, it is the accountability of both processors and controllers to ensure the correct procedures are followed.

2. **Transparency**

   Organisations will have to be open and transparent about why they are collecting personal data and what they intend to do with it. This means explaining to the data-subject what they intend to use their data for upfront and gaining consent.

3. **Processing personal data**

   Personal data can only be collected for specified, explicit and legitimate purposes, and not processed in any further capacity that doesn't meet these purposes. Consequently, data legitimately gathered for one purpose cannot then be used for another objective unless they gain consent from the data-subject or have a legitimate purpose to do so.

4. **Right to access**

   Data-subjects have the right to access their personal data within 30 days of a request. Organisations have a responsibility to ensure inaccurate data is updated or erased; giving data-subjects the right to verify and amend personal information that is held on them.

5. **Right to be forgotten**

   Data-subjects also hold the right to request that his/her personal data is removed, provided that there is no legitimate grounds for keeping it.

6. **Data protection by default (Privacy Impact Assessment)**

   GDPR calls that we evaluate the amount and length of time for which we hold personal data. In circumstances that pose high risk, a Privacy Impact Assessment may be required. It also states that if personal data is gathered on an individual, the organization should not collect any data in excess of what is necessary for the purpose intended.

7. **Fines for impacting privacy or breaching rights**
   Fines of up to 4% of annual turnover or 20 million euros, whichever is higher, could be imposed for breaches of GDPR.

8. **Reporting breaches**
   In the event of a data breach which could impact the individual or cause harm, the data-controller is required to notify the supervisory authority of a significant breach no later than 72 hours after the data breach was detected.

GDPR and Creditsafe

Creditsafe as a business has a requirement to collect data on businesses and their historical conduct in order to assess the creditworthiness of companies. Creditsafe provides its clients with data to allow them to make financial decisions and manage business risks. Personally Identifiable Information (PII) which is handled by Creditsafe is only of those individuals who are directly connected to a business entity[1].

Creditsafe operates in a business to business (B2B) environment and has the PII of individuals either as part of an organization such as a director or as a Sole Trader where by the individual is the business. Creditsafe is only assessing the capability of the business entity to conduct and continue to conduct business and fulfil contracts based on current and historical performance. As such, the type and quality of data provided to customers will not change after the introduction of GDPR.

Where data collected by Creditsafe has been determined as unsuitable for use or does not appear to have appropriate consent this data will then be deleted.

Legitimate interest to deliver information services

GDPR Article 6:F permits the processing for the purposes of the legitimate interests pursued by the data-controller or by a third party. It further states that data-controllers can process personal data without given consent if there is genuine and legitimate reason. This can include commercial benefits, 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-controller relationship

Creditsafe has many different product offerings that clients can choose from. Creditsafe is using its own database to provide the services and can decide what else it uses the data for. Creditsafe will be acting as a data-controller, this position will be covered in the standard Terms and Conditions.

Creditsafe is acting as a data-controller whenever it provides services to the client: Creditsafe is using its own data which it can decide what to do with; it has flexibility to decide how to carry out the task, what data to include and what is important in terms of compiling the report. This will mean that Creditsafe will be wholly responsible for all of its processing activities and must ensure that it only shares personal data when it is lawful to do so.

Any data that Creditsafe provides in our products and services will give rise to a controller-controller relationship with our customers for which *no processing clauses are required*. Despite there being a 'controller-controller' relationship with customers, Creditsafe includes the data protection clauses in our standard customer terms and conditions.

[1] Creditsafe's business in Sweden and Norway also collect and process data on consumers under the provisions of credit reference laws.

As a controller, Creditsafe must ensure that it only shares personal data when it is lawful to do so and therefore Creditsafe sets out in the terms and conditions the framework for the sharing of personal data and an acknowledgment from the customer that in order to use our services they must have a lawful basis for doing so. In the terms and conditions of Creditsafe there is a list of the reasons a customer can use our products.

Some specific information services are:

Search input

The non-binding view of the DPA was that the search terms are irrelevant – the company owning the database was a data-controller of the database and when it sent information to the customer by way of a report, the customer would become a data-controller of that report. Therefore, it is a matter of whether or not you can lawfully share information in the first instance.

Data cleanse/ append and Trade Payment data

Creditsafe is 'controlling' what corrections are being made to that data and what additional information/data is to be appended as part of the service. Creditsafe has the flexibility to decide how to carry out the task, we are a 'controller' of that data.

Can our customers use our information?

Yes, all of our data and products are aligned with the requirements and we are both using data in line with consent or legitimate interest.

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. 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 GDPR.

creditsafe

How Creditsafe has aligned with GDPR

Creditsafe has taken a total business approach to GDPR and reviewed all business and data processes to ensure that they align with the legitimate interests of our business to support customers in making 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 storage (data mapping)

For all stages of data custody we look to identify 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. 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.

Understanding our data uses

When data has been collected, such as legitimate interest, records of processing, or consent, Creditsafe ensure that data is adequate, relevant and not excessive in relation to the purpose. Creditsafe systematically assesses its data to verify legitimate interest.

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 be Forgotten (R2BF), data correction, change of consent where it has been given, and moving data to another platform for individual use.

Data integrity and transparency

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.

Implementing appropriate technical and organizational measures

To protect data against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data, Creditsafe are implementing technologies which will allow us to firstly identify and then tag sensitive Personal Identifiable Information (PII), resulting in all data being protected. This ensures that the data is not misused or removed outside of the Creditsafe network through unauthorised actions.

Here are some of the measures we take to protect our systems and data:

- 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, automated alerts and alarms in place.
- Antivirus – All compatible endpoints covered by antivirus software, with automatic updates via an update server and the Internet.
- 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 Loss Prevention: Creditsafe has implemented controls to protect data from leaving its network unless authorised both over networks and via external media sources.

Implementing appropriate controls

Creditsafe operates to avoid data transfers to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data-subjects in relation to the processing of personal 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. It is also being used in our business strategy, ensuring all future business decisions and developments consider the impact on the individual before we go forward.

creditsafe

FAQ's

Are Creditsafe fully GDPR compliant?

Creditsafe are engaged in a full GDPR program ensuring that both our operations and services are in full alignment with the regulation.

Creditsafe as a business has a requirement to collect data on businesses and their historical conduct in order to assess and provide its clients with data to allow them to make financial decisions and manage business risks. PII which is handled by Creditsafe is only of those individuals who are directly connected to a business entity.

Creditsafe operates in a business to business (B2B) environment. Where we have the PII of individuals either as part of an organization such as a director or as a Sole Trader where by the individual is the business. We are only assessing the capability of the business entity to conduct and continue to conduct business and fulfil contracts based on historical performance. As such, the type and quality of data provided to customers will not change after the introduction of GDPR. Where data collected by Creditsafe has been determined as unsuitable for use or does not appear to have appropriate consent, this data will then be deleted.

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, regulated by the FCA and registered as a data-controller with the UK Information Commissioner's office.
- Creditsafe operates through a Tier3+ UK datacentre, 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, automated alerts and alarms are also 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.
- Bata 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.

Creditsafe Marketing Data

How are Creditsafe preparing their marketing data for GDPR?

Creditsafe are engaged in a full GDPR programme ensuring that all data is collected and used under proper permission, be that consent or legitimate interest. Usage of data is fully mapped throughout the business and subjected to rigorous risk and data privacy impact assessments.

What consent does Creditsafe ask from the businesses we collect information from?

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 6:F 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.

Where is all the data we access hosted, is this the UK?

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