GDPR Guidance

The information contained on this page is for general guidance purposes only. It should not be taken for, nor is it intended as, legal advice. We would advise customers to seek their own legal advice if they are unsure about the implications of the GDPR on their businesses.

1. Introduction

This document is intended to assist you with your GDPR compliance requirements by explaining what type of personal data Credit Hound Cloud is processing and how such personal data may be processed by you acting as a “Controller” and Draycir acting as a “Processor” (including other sub-processors). This may assist you in ensuring that your records are compliant with GDPR, however you must also make your own assessments.
Should you have any questions that cannot be clarified within this document please contact our Support Desk via email on support@draycir.com.

2. The purposes of your processing

As a Controller it is up to you to determine the purpose for which you are processing personal data but Credit Hound Cloud is typically used for the following purposes:

- The provision and management of financial and accounting information;
- The provision and management of customer account information;

Also, it is up to you as the Controller to determine as to what lawful basis you wish to rely upon to process the user’s personal data.

3. A description of the categories of individuals and categories of personal data

Credit Hound is designed to hold data on the following categories of individuals:

- Customers

Credit Hound Cloud has the ability to hold the following categories of personal data:

- Customer identification data – such as the customer’s; reference, first name, last name, address information, post/zip code
- Account identification data - such as the user’s: first name, last name, email address and username. This information is the minimum level required in order to ensure that Credit Hound Cloud is able to track and record the activities within the software.
- Chasing for debt - Customer contact details are shown in order to pursue any outstanding invoices or following up on disputes.
- Customer Activity - Records and stores actions and all correspondences sent to Customers.
- User Management Captures all user details that require & have access to Credit Hound Cloud.
- PayThem - Credit Hound Cloud provides the facility for end users to add a clickable button on the outbound emails, to allow customers to pay invoices using a Payment Provider such as; Total Processing, Elavon and Stripe. The recipient’s name, address and email address are required in order to provide this service.
- Credit Reports – Credit Hound Cloud offers Clients the option to purchase Credit Reports. Upon purchase, we obtain Commercial Credit Data from Experian to produce these Reports. This data may include personally identifiable information of your customers, such as identification details for Directors, Shareholders, and Secretaries.

4. Recipients of personal data

In providing the Credit Hound Cloud service, the following third parties have access to data:

- Hosting service:
    - o Microsoft in the provision of its Azure services.
- Emailing service
    - o SendGrid in the emails that are sent and received to your customer contacts when chasing for debt.
- We use Hotjar in order to better understand the users’ needs and to optimize our services and user experience. Hotjar is a technology service that helps us better understand our users’ experience (e.g. how much time they spend on which pages, which links they choose to click, what users do and don’t like, etc.) and this enables us to build and maintain our service with user feedback. Hotjar also uses cookies and other technologies to collect data on users’ behavior and their devices. This includes a device's IP address (processed during a user’s session and stored in a de-identified form), device screen size, device type (unique device identifiers), browser information, geographic location (country only), and the preferred language used to display the website. Hotjar stores this information on our behalf in a pseudonymized user profile. Hotjar may retain the IP address information for thirty calendar days before de-identifying or deleting it. Hotjar is contractually forbidden to sell any of the data collected on our behalf.

- If using the Funding Search functionality in Credit Hound Cloud, Draycir introduces customers to Capitalise, who help UK firms access business finance, working directly with businesses and their trusted advisors. Capitalise.com is a credit broker and not a lender. Capitalise are authorised and regulated by the Financial Conduct Authority. Draycir's relationship with Capitalise is limited to that of a business partnership, no common ownership or control rights exist between us.

By continuing you agree to all Capitalise's terms and conditions.

- Payment Providers
    - Via the PayThem service.
- Payment Service and Billing Management
    - With Chargebee.
- Authentication and User Management
    - With Auth0.

5. Data Location

Credit Hound Cloud data is stored in either the United States in the Central US data centre, or in the United Kingdom in the UK South data centre, operated by Microsoft.

The email delivery service used is provided by SendGrid which is a third party service, whose data centres are based in the United States. [https://sendgrid.com/resource/general-data-protection-regulation-2/]

For identity management, the authentication and authorisation services are provided by Auth0, which is a third party service, whose data centres are based in the EU. [https://auth0.com/docs/compliance]

To help us better understand our users and maintain our service through user feedback, we use Hotjar, which is a third party service, whose data centres are based in the EU.
[https://www.hotjar.com/legal/compliance/gdpr-commitment/]

We use Chargebee as a payment service and for billing management, whose data centres are based in the EU. [https://www.chargebee.com/docs/2.0/eu-gdpr.html]

As part of Chargebee, we also use GoCardless to process Direct Debit payments, whose data centres are based in the EEA. [https://gocardless.com/legal/gdpr]

PayThem data is stored in Draycir’s cloud repository (hosted by Microsoft Azure in the UK) to allow payments to be made via the PayThem payment portal. Note: Draycir does not hold bank or card payment details. These are solely managed by the payment provider you choose to use with this service.

In order to improve our services or provide additional support, data may be accessible by our subsidiary company Draycir Thailand. The physical data will still be located in UK data centres.

In providing support services, log files may be transferred to Draycir Thailand which may contain some personal data. Such transfers are subject to an approved Data Processor Agreement. Our contact point for any question or complaints in respect of such transfers is support@draycir.com.

6. Retention schedules

Credit Hound Cloud by default logs all activities within the software and retains this information for your security and auditing purposes.

In respect of PayThem - data is retained to provide the payment facility and to maintain an audit history of payments. If you do not wish for your data to be held in the cloud repository, you would need to cease to use PayThem. Should you wish for your data to be removed from PayThem, please let us know via support@draycir.com.

Upon cancellation, termination or non-renewal of the contract, any personal data in Credit Hound Cloud is retained for 90 days before such data is deleted.

7. Technical and organisational security measures

Credit Hound Cloud is a cloud-based solution built on Microsoft Azure services. Microsoft Azure have over 90 security and compliance options to choose from, more information around compliance can be found on the Microsoft Azure website: https://azure.microsoft.com/en-gb/overview/trusted-cloud/compliance/

All our Microsoft Azure services and data are hosted in a secure Data Centre either within the United States or United Kingdom, where access to any of the resources are restricted to key personnel requiring multi factor authentication.

All data is encrypted at rest and is securely transferred using Transport Layer Security (TLS) so that the content of the communication cannot be understood if intercepted. Where the data can only be accessed via a secure authentication mechanism. Access to this data is audited and monitored for threat detection.

Draycir considers its security measures to be appropriate under applicable data protection legislation. Draycir also performs regular auditing of assets in Microsoft Azure to ensure that best practices are maintained and security features of products and services used are enabled.

8. Processor contract

For Customers in the European Union or the United Kingdom, the terms and conditions for the provision of Credit Hound Cloud contain all the provisions required by GDPR or UK Data Protection Legislation, as applicable, in the contract between a Controller and a Processor of personal data.