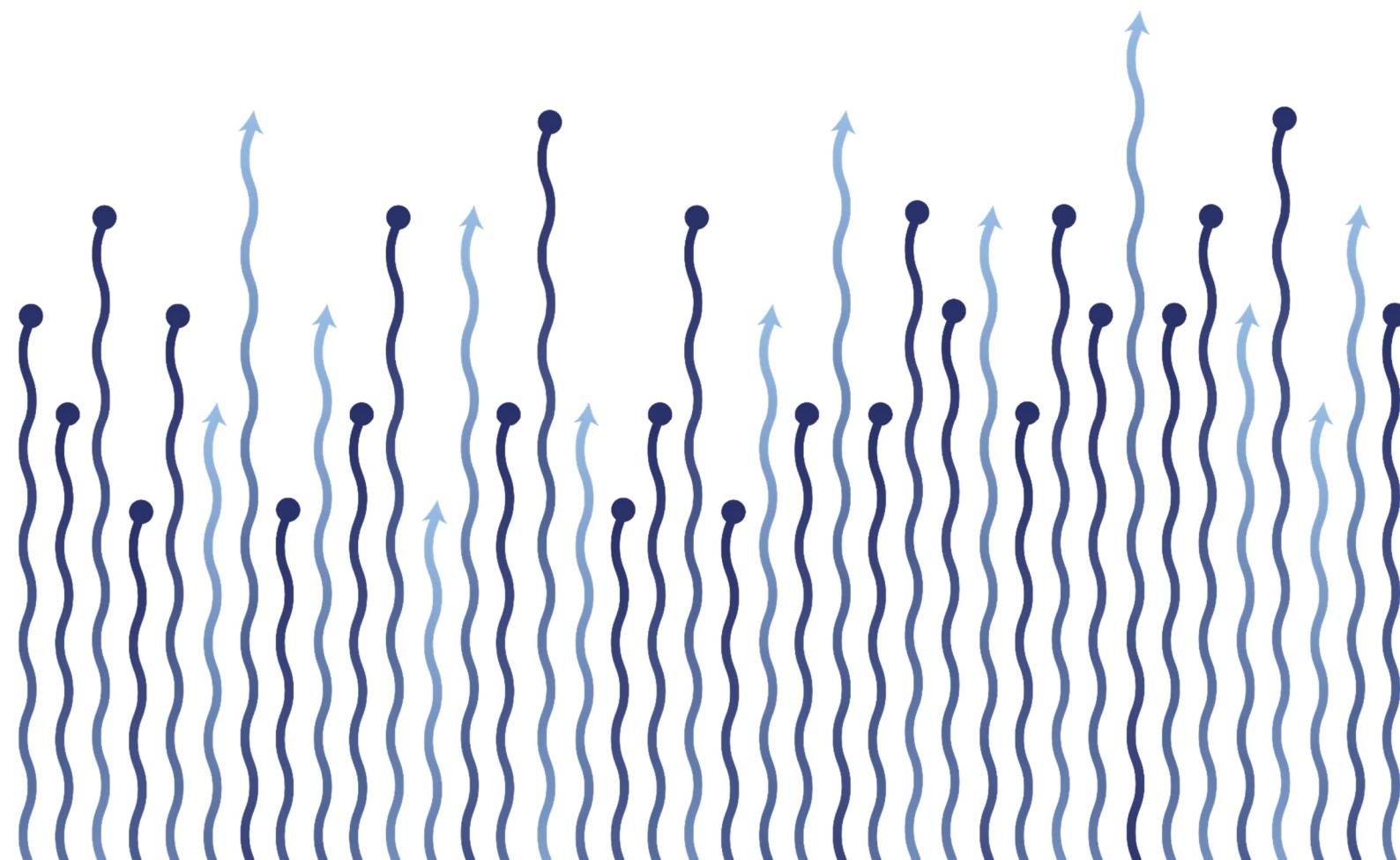




Company Privacy Notice

UPDATED AUGUST 2023

1. What is GDPR
2. The kind of information we hold or have access to and the legal basis that we rely on to process that information
3. Use of Data or Access
4. Security of Data
5. Data Retention and Deletion Policies
6. Third Party Sharing of Data and marketing
7. Location of Data
8. Consent for use of Data and exercising your legal rights
9. Clarification of role – Data Controller or Processor
10. Data Protection Officer
11. Procedures in the event of a data breach
12. Contact Us



1. What is GDPR?

The General Data Protection Regulations (GDPR) and the Data Protection Act 2018 is about ensuring that any personal data held by any institution is kept, with the consent of the individual, for a legitimate purpose only for as long as necessary, and that procedures are put in place to safeguard the security of that data.

Dalacor Ltd only stores data that is required to provide a service to clients. The information is stored securely and obsolete data is removed using a controlled data retention policy.

This Privacy Notice serves as documentation providing transparency for how Dalacor Ltd accesses, uses and secures your data, as well as the length of time the data is kept. References to 'we' 'us' 'our' or Dalacor Ltd means Dalacor Ltd, registered in England and Wales with company registration number 09513959.

2. The kind of information we hold or have access to and the legal basis that we rely on to process it:

Legal Basis

Unless otherwise stated in this policy, the legal basis that we rely on to process your personal information is for our legitimate interests so that we can perform our contract with the Client and provide the relevant services to the Client. We may also process your personal data as it is necessary for our legitimate interests (e.g. to recover any debts due to us) or because we need to comply with a legal obligation (e.g. to notify you of changes to our terms of business).

IT Support

Dalacor Ltd employees have access to all non-encrypted files stored within all folders on the client's Servers.

Dalacor Ltd only accesses files/folders on the server with the explicit instruction from an authorised person, for the sole purpose of providing IT Support.

For IT Support Contracts, we do not host, control, or process any data. All data is hosted, controlled and processed by the Client. Data is electronic, mainly Word, Powerpoint, Excel and Pictures stored in the UK on client's servers.

Thus, we have no category of information listed for IT Support as the information is owned, collated and processed by the client.

Helpdesk System

Contains inventory information (hardware and software), quotes, Purchase Orders and Invoices, IT Support related requests, IT Visits Calendar, Reporting functionality (for financial and IT Support related queries).

First Name, Surname and Email address. Electronically stored in a MySQL Server Database. Stored and backed up in the UK.

Category of Information for helpdesk system: - Personal Data (First Name, Surname and Email Address)

Backup Service

Electronic, Encrypted back up stored in the UK. Dalacor Ltd processes the data for the purpose of backups. Dalacor Ltd is not the Data Controller and therefore have no records of what data contains.

Thus, we have no category of information listed for Backup Service as the information is owned, collated and processed by the client.

Email Correspondence

IT Support Requests and Quotes, Orders and Invoices.

Electronically in .dat file format for email and stored in the UK. This will be moved over to the new CRM Helpdesk in April 2020.

Category of Information for email correspondence: - Personal Data (email address, first name and surname).

Broadband Filter Service

Logs times, user group, website visited, access approved/denied, Google Search terms etc.

The logging service does not store logon passwords nor does it store any information from the webpage.

Format Electronic Text based files, stored in the UK on client's sites. Reports will be imported onto Server hosted by Dalacor Ltd. Server location is UK based.

Category of Information for Broadband Filter Service: - Personal Data (Websites, Google Search terms)

Email Provider Service

First Name, Surname, Email Address, Contacts and Calendars and all the sent and received emails. Date and Time of sent/received emails.

Dalacor Ltd enables clients to access their emails by providing a mail server system (Mdæmon), storage space, as well as Email IT Support.

Dalacor Ltd only accesses files/folders on the server with the explicit instruction from an authorised person, for the sole purpose of providing IT Support and for general maintenance of the mail server

Format Electronic Text Based files, stored in UK

Category of Information for Email Provider Service: - Personal Data (Name, Surname, Email Address, Contacts and Calendars)

3. Use of Data Or Access

IT Support

Provide IT Support for Client's Servers, desktops and laptops.

Dalacor Ltd only accesses files/folders on the server with the explicit instruction from an authorised person, for the sole purpose of providing IT Support.

Helpdesk System

Manage IT Job Requests, Provide Hardware and Software Inventory for asset management purposes. Includes a technician's visits calendar. Manages IT Budget and Finance History. Provides a hardware equipment replacement schedule. Enables you to access relevant information about your network.

Backup Service

At request of client, data is backed up in the event of Server failure, virus, malware or hacking breach. This is a secure encrypted copy of the data.

Email Correspondence

Current Use of Email system is for Quotes, Orders and Invoices and dealing with IT Support Requests. This is being moved to the new CRM Helpdesk system.

Broadband Filter Service

Provide information to assist in safeguarding, malware and virus prevention, including troubleshooting.

Email Provider Service

Storing emails, contacts, calendars to provide an email service to end clients. Dalacor Ltd only accesses this information for the process of storage on behalf of clients.

Use of email logs to eliminate spam, malware and viruses and troubleshooting email delivery issues.

4. Security of Data

We have put in place commercially reasonable and appropriate security measures (including but not limited to encryption, backups, user controlled access) to prevent personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to personal data to those employees, agents, contractors and other third parties who are authorised.

5. Data Retention and Deletion Policies

Dalacor Ltd will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying our legal accounting or reporting requirements. Further information regarding our deletion and retention procedures and "Right to be forgotten" can be found below within our Data Retention and Deletion Policies Document.

IT Support

Server File Structure enables staff to separate data from documents (Data is people related information and documents are non-people related information).

The file structure is a curriculum year hierarchy, which enables easy deletion annually
Dedicated staff are provided with permissions to remove users and the data from the system.

Helpdesk System

Dedicated staff are provided with permissions to deactivate users and remove email address
All other information on the helpdesk system is kept indefinitely as there is a legitimate purpose to retain the information and it is not personal data.

Backup Service

Upon termination of back up service contracts, all backups for the client will be deleted within 30 days.

Email Correspondence

Emails older than two years are deleted
A complete record of all correspondence and easy deletion

Broadband Filter Service

Logs are live for one year. Previous years are archived, encrypted and deleted after five years.

Email Provider Service

If requested, Dalacor Ltd can implement an email retention and deletion policy service
Dedicated staff are provided with permissions to remove users and the data from the email system.
Email retention and deletion policies will be managed separately for legal reasons.

6. Third Party Sharing of Data and Marketing

Dalacor Ltd does not share any personal data with any third parties or use any personal data provided by a Client for marketing purposes (unless consent is otherwise obtained). We do share logs for the following troubleshooting purposes.

Mdaemon support staff may view relevant anonymised email logs
The relevant third party for those specific products provided by them, may view any logs used by clients that require support from a third party.

We do not share data for any other purpose.

Dalacor may obtain personal data from approved third parties that provide marketing services to it.
We currently work with Pink Spaghetti who are a marketing company that carry out telesales.

7. Location of Data

All data is hosted within the UK with the following exception:

An encrypted back up of Email, Contacts and Calendars is stored in Zurich, Switzerland by Rsync.net. The EU recognises Switzerland as meeting compliance with GDPR Section 5, articles 44-50.

Our Backup and Email Service is hosted in a UK based secure Tier 4 Data Centre fully protected from theft and fire. It has multiple broadband redundancy to ensure uptime. All your emails are stored as locally as you can get it.

No personal data is transferred outside the EU.

8. Consent for use of Data and exercising your Legal Rights

Service Contracts will constitute consent for use of Client data for the performance of the contract with you.

You will not have to pay a fee to access your personal data (or to exercise any of your other rights as set out below). However, Dalacor Ltd may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive or, may refuse to comply with your request in these circumstances.

Dalacor Ltd may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. Dalacor Ltd may also contact you to ask you for further information in relation to your request to speed up our response.

Dalacor Ltd will try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, Dalacor Ltd will notify you and keep you updated.

You have the right to:

Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data that we hold about you and to check that it is lawfully processing it.

Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.

Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us to continue to processing it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.

Object to processing of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing

purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms.

Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios: (a) if you want us to establish the data's accuracy; (b) where our use of the data is unlawful but you do not want us to erase it; (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

9. Clarification of role – Data Controller or Processor

A data controller determines the purpose for which any given personal data is used.

A data processor processes personal data on behalf of a controller, for example a service provider hosting data or sending out emails on their customers' behalf.

They have differing responsibilities under data protection law.

Neither

IT Support

Data Controller

Helpdesk system, Email Correspondence, Broadband Filter Service and Milelogik Mileage Logger.

Data Processor

Backup Service and Email Provider Service.

10. Data Protection Officer

A data protection officer is required under the following conditions:

1. you are a public authority or body (except for courts acting in their judicial capacity)
2. your core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking); or

3. Your core activities consist of large scale processing of special categories of data or data relating to criminal convictions and offences.

As none of these conditions are relevant, it is hereby recorded that Dalacor Ltd does not require a data protection officer.

11. Procedures in the event of a data breach

For data where Dalacor Ltd is the Data Processor, Dalacor Ltd will take the following steps:

1. Determine whether a breach has occurred
2. Identify the point of failure responsible for the breach
3. Report or Confirm the breach to the appropriate individual who is the Data Controller
4. Advise the steps to be taken to prevent a future breach of that nature

For data where Dalacor Ltd is the Data Controller

The above four steps will be taken in addition to the following:

1. Determine whether there has been a security breach or data breach
2. Should it be decided that personal data (data breach) is compromised then the ICO will be informed within 72 hours and where appropriate, the affected data subject.

12. Contact Us

If you have any questions regarding this privacy notice or if you would like to speak to us about how we process your personal data, please feel free to reach out to our dedicated Data Protection Officer at hello@dalacor.co.uk.

You also have the right to make a complaint to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues, at any time. Website – <https://ico.org.uk/concerns>