GDPR and MindaClient

Helping you become GDPR compliant

Requirement under GDPR	What this means	What MindaClient will do for this requirement
Legal basis for processing personal data	You now need to have a legal reason to process data. You have to recordthe legal basis for processing data. That reason could be consent, part of acontract or what GDPR refers to as "legitimate interest"	MindaClient has added a new field on the client profile screenwhere you can record the legal basis for processing the clientsrecord. This filed is audit tracked in case the basis for processingever changes
Consent Management	A fundamental principle of GDPR is that the person has given you permission to process their data or has given you consent. This is also referred to as Opting in.	When you add a new client you can tick to record that the person has consented to you processing their data.
Informed of right to Object	Under GDPR the person must be informed of the right to object to having their data processed. This could be on a registration form for example	When you add a new client you can tick to record that the person has been informed of their right to object to having their data processed

Objection to processing data	A person or “Data subject” has the right to object to having their data processed.	MindaClient has a facility on the client processing screen to record that the person has objected to you processing their data. Once you tick this then the three permission tickboxes for sending emails, sending texts and printing labels for that person will be automatically cancelled. If the person has just objected to receiving communication by text for example then you can simply untick the “Receive SMS” tickbox for that person.
Block on Processing	If a person has indicated that they no longer wish to have their data processed then you should never be communicating with them.	Once the box is ticked for a client or contact that they no longer wish to have their data processed, then MindaClient automatically blocks out the facility to send emails, send texts or generate labels for this person.
Consent management for existing clients	It may be that your existing clients have already opted in and given consent to you being allowed to process their data	MindaClient lets you filter existing clients and update their consent options in bulk in the Edit Records section

Ongoing Consent	GDPR states that consent lasts for only 12 months. However if you have been communicating with your clients and have given them the option of opting out then this is seen as updating consent.	MindaClient lets you record when you get consent from your clients and it will automtaically update that you have updated this consent as you send out communcation to your clients with the option of opting out.
Withdrawal of consent or facility to opt out	Your clients need to have the option of withdrawing consent or Opting out	MindaClient have built in the facility in the Client Reporting Marketing section to include Opt outs with text and email communications you send to clients. You can also manually withdraw consent if you are get a separate request from a client
Use of Cookies	It is a requirement that users of websites and MindaClient are informed if cookies are being used.	When you first log into MindaClient you are informed that MindaClient uses cookies and you are asked to consent to the use of cookies.

Anonymising Data	Article 17 of the GDPR regulations states that a person has the right of erasure also known as “The right to be forgotten”. It states that they have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay	MindaClient has built a facility that lets you anonymise the personal information relating to both clients and contacts. You just enter the name of the person and it will display all instances of that person in MindaClient. You can then click to anonymise the person. There are checks and confirmations in place to ensure that data is never anonymised without user express confirmation.
Data Retention	Under GDPR you are meant to only hold data for as long as it is required. The retention period will vary depending on the type of company and the type of data and it should be outlined in your GDPR policy. There may be legal or regulatory reasons prescribing how long you need to retain data so you should seek advice irt this area.	You can enter a date in MindaClient and display all the clients you have not contacted since that date. You then have the facility to permanently delete these clients.
Deletion of Data	GDPR requires that you may have to permanently removea client or contact from your database, including, call records, meetings, emails, texts etc.	MindaClient has updated its delete function so that all client data will be cleared and the record is no longer stored in the archive.

Access / Portability	A person can request access to any personal data you hold about them. Personal data is anything that will identify the person such as their name, address and email address. If they request access, you (as the controller) are required to provide a copy of the data to them. They can request it in digital format.	MindaClient have developed an easy to export facility for each client. It will download the clients record to a CSV file which is one format mentioned by GDPR.
Modification of a persons data	A person can ask you to modify their personal data if it's inaccurate or incomplete.	You can firstly record that you got the request to change the data in the GDPR request section. You can modfy their record and the audit trail will record the old and the new values of the record.
Data Cleansing	Article 5 of the GDPR regulations requires that personal data shall be accurate and, where necessary, kept up to date	MindaClient provides a number of functions to help keep your data cleansed on a regular basis. It prevents duplicates when you are adding in new clients or bulk importing. It lets you merge clients if you do come across two clients that both relate to the same company You can carry out bulk updating on clients. For example you could update a batch of clients to be archived at the end of the year.

Restricting Access to your data	The processing of client data is an area that is given much coverage under GDPR. It is very important that only the appropriate people in your organisation have access to your client data.	MindaClient provides a comprehensive facility where you can set access rights for users, ranging from full administration rights to all data, right down to read only or mobile only access rights. There is a record of user access to the system that the administrator can see and there is an audit trail running throughout MindaClient.
Protecting your data from staff	As a data controller you are required to implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the GDPR regulation	There are three points in MindaClient that address these concerns. There is an audit trail running in MindaClient that tracks changes made by users. In the main Client Reporting screen if a user downloads any client information the audit trail record details of the download. If a user is leaving your company, you instantly tick to make them inactive and that removes all access from that user.

Is my data held within the EEA European Economic area	There are additional areas that need tobe addressed if you data is processed outside of the European Economic Area. These would include being satisfied that the country in question where the data is being processed provides an adequate level of data protection.	All MindaClient data is stored within ISO27001 certified data centres in Dublin and will never leave the Irish Jurisdiction. So for current and future data protection regulations and compliance requirements, customers will always know exactly where their data resides.
Recording of Requests	A person has a number of requests they can make to you as a controller such as right to be forgotten, right to amendment, right to stop processing, right to a copy of their personal data. You need a system to record all of these requests.	MindaClient have built in the facility to record all requests received opposite each client. You can record the person submitting the request, the person who records the request and the date of the request.

Management of Requests	As well as recording the requests you need a system to manage the requests to ensure that the request is dealt with within the required 30 days.	MindaClients GDPR management system lets you set reminders when you get requests to ensure that you respond within the timeframe. You can set a reminder for a number of days before the time expires and you will get an email reminder prompting you to check you have responded. When you reply to the request you will have a record of this response as well.
Audit Trail	From a security point of view you should be able to answer the following questions “Who accessed or changed data within our systems?” “When was the data accessed or when was it changed?” “When did a specific user last access to the system	There is an audit trail running in MindaClient and this tracks all changes by users. It records The person who added the record The value before the change was made The person who made the change The date and time of the change The new value of the data It records when a user accessed MindaClient

Security Measures	The GDPR brings in a number of new and increased data security requirements relating to data in transit and data at rest	The following is a summary of the security steps that MindaClient has undertaken. **Encryption** All data transferred to and from our websites is encrypted via HTTPS using strong SHA-256 bit encryption. Similarly, all backups between servers are made using SHA-256 bit encryption. **Constant Back up** A full backup of the MindaClient server is made every hour using a secure SSH encrypted connection between servers. This is done using an automated and dedicated backup service located within the Irish Republic.

Firewall

Our MindaClient server has a hardware firewall at datacentre level, and in addition there is a software firewall on each machine. Access over all ports is fully restricted based on the need to access, and when access is allowed, this is further restricted based on IP address.

Failover

Our MindaClient server is mirrored in real time to a failover server on the AWS cloud (Dublin). In the unlikely event of a disruption to service on our primary server, we have an IP switching service in place that will allow us to simply failover to the secondary machine.

Hashed passwords

All passwords are hashed. In the event of a breach, none of our user passwords can be decrypted.

Strong passwords

We have implemented a ‘strong password’ policy. When creating a password, this strong password criteria must be met by users.

Regular Updating of Passwords

We have an automated facility that allows our clients to turn on the forced updating of their users’ passwords. When a set time period has elapsed, the user will be required to change their password to a new ‘strong’ password.

Password Reset

If a user needs to reset their password, they can make this request on the login page of our website. An email is sent to the registered email account of that user, allowing the user to update their password securely.