GDPR Compliance

Web Hosting

Some of our hosting had been in the UK. If the data is not hosted within the EU then there is a strong onus to satisfy ourselves that the external country is complying with the requirements of GDPR. We believed that hosting within Ireland would give our customers confidence with the data being stored within ISO27001 certified data centres in Dublin and the guarantee that data will never be hosted outside the Irish Jurisdiction.
Our data is hosted in BT Ireland Centre, at City West Digital Park, Dublin with company BT Ireland Managed Service, Grand Canal Plaza, Upper Grand Canal Street, Dublin 4.
They have been awarded the following standards.

ISO 27001 : 2013

ISO 9001 : 2008

ISO/IEC 20000 – 1:2011

MindaClient Security

1. Data Centre

Our servers are all located in Ireland, including all offsite backups and failover services. The data centre we use has Tier III data centre classification and ISO 20000/9001/14001/27001 certified.

2. Firewall

Our MindaClient server is protected by physical and a software firewalls. Traffic on all ports is tightly restricted. Access, where appropriate, is locked down by IP address.

3. User Access Control Management

Access to the server is severely limited. Only the MindaClient Development team have access the server or the database. Direct access to the server is restricted to our office IP address, and a strong password policy is observed. Our server management company may also, with our permission, access the server to perform upgrades and server administration.

4. Password Policy

It is the policy of SalesPulse / MindaClient that all passwords are unique, and complex (meeting the ‘strong password’ standard). All passwords are changed on a quarterly basis.

5. Software Updates

Updates and security patches are installed regularly by our server management team.

6. Encryption of Personal Data in Transit

All data transferred to and from the website is encrypted via HTTPS.

7. Intrusion Detection and Prevention

In addition to our physical firewalls, we use intrusion detection and prevention tools to monitor and control all traffic to and from the website. We also have external detection and mitigation on the network for DDOS attacks.

8. Failover

We use real-time data replication and server-to-server synchronisation to maintain an independent failover of the MindaClient service. In the event that the primary MindaClient server becomes unavailable, we have the facility to failover to our secondary system in order to maintain availability.

9. Data Backup

The MindaClient database is backed up automatically every 60 minutes, 24/7. The backup is from secure web server to secure web server over SSH, so all data is fully encrypted end to end during the backup process. The backups are accessed through a secure portal using a strong password.

Data Protection Commissioners Requirements

The Data Protection Commissioner produced a comprehensive checklist for companies. The following outlines the work we have carried out to make us compliant with GDPR:

Data Breach Response Plan

This plan outlines the steps MindaClient will take if there is a Data Breach.

Security Complaints Procedure

This procedure lays out the procedure a staff member must follow once they receive a complaint.

Data Breach Notification Template Form

There are two sections in this template, each having a number of questions that must be answered in the event of a Data Breach.

The timeframe for reporting and the address to be communicated with are included in this template.

Subject data breach notification

If the breach is likely to adversely affect the personal data or privacy of your subscribers or users, we need to notify them of the breach without unnecessary delay. This section outlines the steps and procedures we must follow.

Privacy Policy

We have re-written our Privacy Policy in accordance to take account of the GDPR requirements. This updated policy is available at the footer on our MindaClient website.

Appropriate technical & organisational security measures

We have documented the technical and security measures that we have put in place in order to comply with the GDPR requirements.

Accuracy

We have put in place procedures to ensure all personal data is kept up to date and accurate.

This involves Individual data checking and checking that can be carried out in bulk with new technology we have developed.

Data Minimisation

The policy of SalesPulse is to ensure that the amount of personal data held by us is adequate, relevant and not excessive. The amount of personal data that we hold is limited to:

- Name of subject
- Telephone number of subject
- Mobile number of subject
- Email address
- Address
- Eir Code

Right to object to processing

The data subject has the right to object to processing based. In this section we outline the steps that we will take if a person objects to having their data processed. We have built in functionality into MindaClient to manage this process.
Right to halt processing
The data subject has the right to obtain from the controller restriction of processing where one of the following applies

- the accuracy of the personal data is contested
- the processing is unlawful
- the controller no longer needs the personal data for the purposes of the processing,

- the data subject has objected to processing pursuant to Article 21(1)

We have put procedures in place to manage this process, including reminders to ensure that the request is dealt with in a timely fashion.

Right to restriction of processing

The data subject has the right to obtain for the controller restriction of processing where one of the following applies

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims
- the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

We have put procedures in place to manage this process, including reminders to ensure that the request is dealt with in a timely fashion.

The right to rectification

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.

We have put procedures in place to manage this process, including reminders to ensure that the request is dealt with in a timely fashion.

The right to erasure (right to be forgotten)

The data subject shall 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 where one of the following grounds applies

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
- the data subject withdraws consent on which the processing is based
- the data subject objects to the processing pursuant to Article 21(1)
- the personal data have been unlawfully processed

- the personal data have to be erased for compliance with a legal obligation

We have put procedures in place to manage this process, including reminders to ensure that the request is dealt with in a timely fashion.

Providing individuals with personal data from MindaClient

A person is entitled to a copy of their data. We have outlined the procedure how this data can be extracted in a digital format and forwarded securely to the data subject.

Subject Access Request (SARS) Policy

A SARS request can be submitted in writing, electronically (e.g. via email) or via traditional post.

Under GDPR regulations, a subject has the right to request and obtain confirmation as to whether their personal data is being processed

The SARS request must be responded to in writing within 30 days of the receipt of the request.

We have put procedures in place to manage this process, including reminders to ensure that the request is dealt with in a timely fashion.

Legitimate Interest

There are a number of reasons that are deemed to be legitimate bases for processing data.

- the data subject has given consent
- processing is necessary for the performance of a contract
- processing is necessary for compliance with a legal obligation
- processing is necessary in order to protect the vital interests of the data subject
- processing is necessary for the performance of a task carried out in the public interest
- processing is necessary for the purposes of the legitimate interests

MindaClient believes that 1(b) and 1(f) cover all instances of our data processing.

We have adapted MindaClient software so that the legitimate interest of processing a subjects data can be recorded opposite every client

Types of Data Collected by MindaClient

We outline the types of data that is collected and processed by MindaClient. This includes

- Current Client Data
- Former Client Data
- Current Employee Data
- Former Employee Data
- Supplier Data

MindaClient Data Retention & Deletion Policy

We have prepared a comprehensive Data Retention and Deletion policy that sets out the timeframes for retention and deletion of all of the following categories of data.

A. Accounting and Finance
B. Contracts
C. Client Records
D. Correspondence and Internal Memoranda
E. Electronic Documents
F. Payroll Documents
G. Pension Documents
H. Personnel Records
I. Tax Records

Contracts with our Suppliers

As we are a data processor we are required to have a contract in place with all of our 3rd party providers in order to demonstrate GDPR compliance.

We have written to all our 3rd Party suppliers and are signing the contracts as we receive them.

Data Processing Agreement

We have written a new Data Processing Agreement which we are providing to our clients. This is a requirement under GDPR.

A templated copy of this available at the footer of our MindaClient website.