Talkplan.com Ltd Privacy Policy

At times Talkplan.com Ltd (We, the Company) need to collect, store, use and share certain information about individuals.

Individuals can include customers, suppliers, business contacts, employees and other people the company has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures that we:

Comply with data protection law and follow good practice;
Protect the rights of staff, customers and partners;
Are open about how we store and process individuals' personal data;
Protect the company from the risks of a data breach

Data protection law

The General Data Protection Regulation (GDPR) describes how we must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not be disclosed unlawfully.

The General Data Protection Regulation is underpinned by six important principles. These say that personal data must:

1. Be processed fairly, lawfully and in a transparent manner;
2. Be collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes;
3. Be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. Be accurate and, where necessary, kept up to date;
5. Be kept for no longer than is necessary for the purposes for which the personal data is processed; and
6. Be processed in a way that ensures appropriate security of the personal data.

People, risks and responsibilities

This policy applies to:

Head office
All branches
All staff and volunteers
All contractors, suppliers and other people working on behalf the company

It applies to any information, provided by you directly, which we hold relating to an individual from which an individual can, directly or indirectly, be identified. This can include but is not limited to:

Names of individuals
Postal addresses
Email addresses
Telephone numbers
Reference numbers

Reasons we can collect and use your personal information

We rely on the following as the lawful basis on which we collect and use your personal information:

Consent
Contract
Legal Obligation
Legitimate Interest

The legitimate interests relied upon are as follows:

The information gathered will be used for legitimate business marketing and customer service which is relevant to the end business user.

Data protection risks

This policy helps to protect the company and individuals from some very real data protection risks, including:

Breaches of confidentiality. For example, information being given out inappropriately.
Excess information collection. For, example collecting more personal information than is necessary for the firm to provide the service.
Failing to offer choice. For example, all individuals should be free to choose how the company uses data relating to them.
Out of date. For example, storing out of date and inaccurate information.
Data retention. For example, keeping personal information indefinitely when no longer in use.
Reputational damage. For example, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Please note that while we will use all reasonable efforts to secure your data, in using our website you acknowledge that the internet is not entirely secure and, as such we cannot 100% guarantee the security of any information that is entered by you via any page on our website. If you have any questions or concerns regarding using our website please contact us by email to the details at the bottom of this privacy policy.

We have taken the appropriate security measures available to prevent personal information from being lost or accessed in an unauthorised way.

Everyone who handles personal information within the company has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

The following people have key areas of responsibility:

The **Directors of the company** are ultimately responsible for ensuring that the firm meets its legal obligations.

The **Compliance Officer** is responsible for:

- Keeping the Directors updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data the company holds about them (also called 'subject access requests').
- Dealing with requests from individuals who want to exercise their rights under GDPR (e.g. request erasure of their personal information)
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data
- Carrying out data protection risk assessments
- Carrying out internal data protection audits
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by the data protection principles.

The **IT team** (either on or off site) are responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure that security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

General staff guidelines

The only people able to access data covered by this policy should be those who need it for their work.

Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.

The company will provide training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

In particular, strong passwords must be used and they should never be shared.

Personal data should not be disclosed to unauthorised people, either within the company or externally.

Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Employees should request help from their line manager or the Compliance Officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT team, Directors or the Compliance Officer.

We will hold your personal information for 6 months from point of contact and consent unless you have entered into an agreement and or contract. In which case your information will be held for the duration of that agreement or contract.

When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

When not required, the paper or files should be kept in a locked drawer or filing cabinet.

Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.

Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

Data should be protected by strong passwords that are changed regularly and never shared between employees.

If data is stored on removable media (like a Data USB, CD, DVD), these should be kept locked away securely when not being used.

Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.

Servers containing personal data should be sited in a secure location, away from general office space.

Data should be backed up frequently. Those backups should be tested regularly, in line with the company standard backup procedures.

Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

All servers and computers containing data should be protected by approved security software and a firewall.

Data use

Personal data is of no value to the company unless it can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.

Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.

Data must be encrypted before being transferred electronically. The IT team and Directors can explain how to send data to authorised external contacts.

Personal data should only be transferred outside of the European Economic Area if the receiving firm has adequate data security measures.

Employees should not save copies of personal data to their own computers.

Always access and update the central copy of any data.

Data accuracy

The law requires us to take reasonable steps to ensure data is kept accurate and up to date.
It is the responsibility of all employees who work with data to take steps to ensure it is kept accurate and up to date.

Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

The company will make it easy for data subjects to update the information it holds about them.

Data should be updated immediately if inaccuracies are discovered. For example, if a customer can no longer be reached on his stored telephone number, it should be removed from the database.

It is the Directors responsibility to ensure marketing databases are checked against industry suppression registers every six months.

Individuals' rights

All individuals who are the subject of personal data held by the company are entitled to:

1. Obtain confirmation about what information we hold about them and to access copies of that information.
2. Request the correction of inaccurate personal information.
3. Request the erasure of their personal information.
4. Restrict how their personal information is used.
5. Receive their personal information in a legible and transferable format. For example, in an Excel format.
6. Stop the use of their personal data.
7. Object to their personal information being used for an automatic decision.
8. Be informed about why their personal information is being collected and how it will be used.

The company must make it easy for individuals to exercise their rights in relation to their personal information. Where an individual makes any of the above requests we must comply within one month.

The company cannot charge a fee to an individual for exercising his rights unless the request from the individual is excessive. For example, because it is a repetitive request that has previously been complied with.

Any charge should be limited to the administrative cost of complying with the request.

The Compliance Officer will always verify the identity of anyone making a request to exercise his individual rights before actioning the request.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the individual.

Under these circumstances, the company will disclose the requested data. However, the Compliance Officer will ensure the request is legitimate, seeking assistance from the Directors and from the company legal advisers where necessary.

Providing information

Ultimately the company aims to ensure that individuals are aware that their data is being processed, and that the individuals understand:

How the data is being used
Who their data is being shared with
How long their data will be stored
How to exercise their rights
How to lodge a complaint with the Information Commissioner's Office

If you have any questions about this policy or the information we hold about you, please contact us by:

Email: info@airtimesolutions.co.uk

Post: Airtime Solutions Ltd
Progress House
Churchill Court
Faraday Drive
Bridgnorth
WV15 5BA

Please note that we may change this privacy statement from time to time. We will endeavour to inform users of any changes by email if it has been directly requested to receive privacy policy updates.