DATA PROTECTION POLICY & PRIVACY NOTICE

Everyone has rights with regard to how their personal information is handled. During the course of our activities it is necessary for us to collect, store and process personal data and we recognise the need to treat it in an appropriate and lawful manner.

As a business, and as an employer, the types of information that we may be required to handle include details of current, past and prospective customers, suppliers, current and prospective employees, workers, and other third parties who we engage to provide services for us, and/or do business with.

This data is subject to certain legal safeguards specified in the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 in terms of the way personal data is kept and used.

This policy sets out our commitment to being transparent about how we collect, use and process personal data and our commitment to data protection, and the rights and obligations in relation to personal data.

If you consider that our provisions for complying with the Act have not been followed in respect of personal data about yourself or others you should initially raise the matter with the HR department by emailing hr@airnavigationsolutions.co.uk. If you are not satisfied, you can make a complaint to the Information Commissioner's Office https://ico.org.uk

Definition of Data Protection Terms

Data is information which is stored electronically, on a computer, or in certain secure paper-based filing systems.

A **data subject** is a living, identified (or identifiable) individual we hold personal data about.

Personal data is data we hold about a data subject. What makes it personal data is the fact that the data subject can be identified (directly or indirectly) from that data (or from that data and other information in our possession or available to us). Personal data can be factual (e.g. a name, address or date of birth) or it can be an opinion about the data subject, their actions and behaviour (such as a performance appraisal).

Processing is a term used to describe what we do with the personal data. It applies to most activities that might be undertaken in respect of the data, such as: collecting, recording, organising, structuring, storing, adapting or altering, retrieving, consulting, disclosing by transmission, dissemination or otherwise making it available, aligning or combining, restricting its use, erasing or destroying it. Processing also includes transferring (or disclosing) personal data to third parties.

A **data controller** is the person(s) who, or organisations which, determine how and why personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.

Data users are those persons whose work involves processing personal data. Data users have a duty to protect the data they handle in accordance with this policy and any applicable data security procedures.

Data processors means any person(s) or organisation that processes personal data on our behalf and on our instruction. Employees of data controllers are excluded from this definition, but it could include suppliers who handle personal data on our behalf.

Special categories of personal data is a term used to describe sensitive personal data, such as information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of,
or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions and will usually require the express consent of the person concerned.

Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

- processed fairly, lawfully and in a transparent manner;
- processed ONLY for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary for the legitimate purpose(s) for which it is processed;
- accurate and kept up to date, ensuring, where reasonably possible, that inaccurate personal data is rectified or deleted without delay;
- not kept longer than necessary to fulfil the purpose(s) for which it was collected;
- processed in line with data subjects' rights;
- be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures, and;
- not transferred to people or organisations situated in countries without adequate protection.

Fair, Lawful and Transparent Processing

GDPR is intended not to prevent the processing of personal data, but to ensure that it is done fairly, lawfully and transparently, without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, the data subject must be told who the data controller is (in this case Air Navigation Solutions) and it must meet at least one of a number of conditions specified by legislation. We haven’t listed all those conditions here, but generally we will process data where it is necessary:

- for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract; or

- for compliance with a legal obligation to which we are subject; or

- in the pursuit of our legitimate interests, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

In addition to the above conditions, we can also process a data subject’s personal data where they have given consent for one or more specified purposes, provided that such consent is a freely given, specific, informed and unambiguous indication of the data subject’s wishes. A data subject will have the right to withdraw any consent given.

For special categories of personal data to be processed lawfully, there are additional conditions which must be met, in addition to satisfying one of the above conditions for processing personal data. Conditions for processing special categories of personal data include:

- the data subject has given explicit consent to the processing of that data for one or more specified purposes; or

- the processing is necessary for carrying out obligations under employment law, social security or social protection law, or a collective agreement; or

- the processing is necessary for the purposes of preventive or occupational medicine, or for the assessment of the working capacity of an employee; or

- the processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or

- the processing relates to personal data which has been made public by the data subject; or

- the processing is necessary for establishing or defending legal claims.

Responsibility for data protection

As a data controller, we are responsible for establishing practices and policies in line with the GDPR and any other laws governing data protection. It is important that we do more than just say that we are complying with data protection laws; we must also *demonstrate* compliance. We will do this by:

- implementing processes and policies that enable us to comply with data protection laws, such as not collecting more personal data than we need, providing comprehensive, clear and transparent privacy notices, and creating and improving security features;

- undertaking data protection impact assessments, where appropriate, when using new technologies where the processing is likely to result in a high risk to the rights and freedoms of data subjects;

- introducing new technical measures (such as new software, hardware, or processes) where appropriate;

- undertaking periodic internal audits of personal data held by us; and

- training staff on their responsibilities under GDPR.

Notifying data subjects

Personal data may only be processed for the specific purposes notified to the data subject in the Privacy Notice contained within this policy which provides information for staff about our reasons for processing personal data, how we use such data and the legal basis for processing.

This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs. Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

Such privacy notices will provide information about:

- the types of personal data we process;
- the purpose and the legal basis for processing their personal data;
- whether the personal data will be disclosed to any third parties in the course of processing;
- whether the personal data will be transferred outside of the EEA and, if so, what safeguards will be put in place in this regard;
- how long the personal data will be processed for or, if that is not possible, the criteria we will use to determine the period. Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required;
- how the data subject can obtain a copy of the personal data held about them;
- details of their rights, including how to make a complaint;
- if the personal data has to be processed in order to comply with a law or a contract, the possible consequences of the data subject failing to provide the data and/or (where applicable) objecting to the processing of it;
- the existence and details of any automated decision-making processes.

Rights of data subjects

Data must be processed in line with data subjects' rights. Data subjects have a number of rights in relation to their personal data:

- request information about the personal data hold about them by a data controller;
- Personal data must be accurate and kept up to date. Any inaccurate, misleading personal data should be corrected or amended and incomplete personal data completed, subject to us satisfying ourselves that the data is in fact inaccurate or incomplete. Steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out of date data should be destroyed.
- object to us processing their personal data where we are doing so in pursuit of our own legitimate interests. We can continue processing the personal data notwithstanding an objection if our legitimate interests outweigh those of the data subject, or if we need to do so for the establishment or defence of a legal claim;
- ask us to destroy personal data about them. We can refuse this request if the personal data is still necessary in relation to the purposes for which it is being processed, and there is a legitimate basis for us to continue processing;
- ask us to restrict the processing of their personal data to merely storing it. This can only be requested if: the accuracy of personal data has been contested and remains unverified, if we no longer require the personal data but the data subject needs it to establish or defend a legal claim, if the data subject has objected to the processing of personal data and we are deciding whether our legitimate interests override theirs, or if our processing is unlawful.

- prevent processing of their data for direct-marketing purposes, and;

- prevent processing that is likely to cause damage or distress to themselves or anyone else.

Where we rely on our legitimate interests as the basis for processing data, we will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

If a data subject exercises these rights and we have disclosed the personal data in question to a third party, we will do our best to ensure that the third party complies with the wishes of the data subject.

If a data subject wishes to take any of the above steps, the individual should send their request in writing to the HR department by emailing hr@airnavigationsolutions.co.uk

Subject access requests

Data subjects have the right to make a formal request for the personal data we hold about them. This request must be made in writing to hr@airnavigationsolutions.co.uk

We will normally respond to a request within a period of one month from the date it is received. In some cases, such as where we process large amounts of an individual's data, we may respond within three months of the date the request is received. We will write to the individual within one month of receiving the original request to advise if this is the case.

If an individual makes a subject access request, we will provide the following information:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;

- to whom their data is or may be disclosed to, including recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;

- for how long their personal data is stored (or how that period is decided);

- their rights to rectification or deletion of data, or to restrict or object to processing;

- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and

- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

We will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless agreed otherwise. In addition, where the request has been granted, we will, where possible, provide evidence that your request has been actioned and dealt with appropriately.

If a subject access request is manifestly unfounded or excessive, we are not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that

is unfounded or excessive, we will notify them that this is the case and whether or not we are obliged to respond to it.

Keeping personal data secure

When we process personal data, we must do our best to ensure that appropriate security measures are taken so it remains secure and is protected against unlawful or unauthorised processing of personal data and against accidental loss, destruction or damage. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

We will do this by putting in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- confidentiality means that only people who are authorised to use the data can access it;
- integrity means that personal data should be accurate and suitable for the purpose for which it is
- processed; and
- availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

We will do this by:

- Entry controls - any stranger seen in entry-controlled areas should be reported;
- Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential);
- Methods of disposal. Paper documents should only be securely shredded in the facility available. Floppy disks and CD -ROMs should be physically destroyed when they are no longer required;
- Equipment - data users should ensure that individual monitors do not show confidential information to passers-by and that they log off/lock their screens when it their laptop/PC is left unattended;
- Ensuring PCs/laptops/personal mobile devices/tablets have a personal password login at all times;
- password protecting personal data where appropriate/possible;
- ensuring the ongoing confidentiality, integrity, availability and resilience of systems and services used to process personal data;
- ensuring the restoration of access to personal data in a timely manner in the event of a physical or technical incident; and
- facilitating regular testing, assessment and evaluation of the effectiveness of technical and organisational measures for ensuring data security.

In assessing the appropriate level of security, we shall take into account the risks associated with the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data that we process.

Erasing or destroying personal data

Paper records that contain personal data will be shredded and disposed of securely when there is no longer a need to retain them. Paper records containing personal data must not be disposed of in any other way.

For electronically stored data, there is a significant difference between deleting personal data irretrievably, archiving it in a structured, retrievable manner, or moving it as unordered data to an electronic wastebasket. Personal data that is archived, for example, is subject to the same data protection rules as 'live' personal data.

When deleting electronic data, all possible steps should be taken to put the data in question beyond use. Where it is impossible to delete data from the electronic ether altogether, all reasonable steps should be taken to ensure that it is deleted to the fullest extent possible.

The IT department will be responsible for erasing electronic equipment that contains personal data (e.g. laptops and desktops) securely.

Transferring data to third Parties

If we need to use third parties to process personal data on our behalf, we will require those third parties to provide us with sufficient guarantees that they have appropriate technical and organisational measures in place to comply with the GDPR and to ensure the protection of the rights of the data subjects.

Transferring personal data outside the EEA

We do not currently transfer data outside of the EEA.

If at any point in the future this changes, we shall only transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

- the data subject has given their explicit consent to the proposed transfer, after we have informed them of any possible risk associated with such transfers (e.g. the absence in that country of equivalent safeguards);

- the transfer is necessary for the performance of a contract to which the data subject is a party, or which is in the interest of the data subject, or to take steps at the request of the data subject prior to entering into a contract;

- the transfer is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or

- the transfer is necessary for the establishment or defence of a legal claim.

For each transfer of data outside the EEA, we will record which of the conditions we are relying on.

Training

We will provide training to all individuals about their data protection responsibilities as part of the company induction process.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Personal data breach

It is very important that we remain alert to the risks of personal data breaches, and that we react quickly to an apparent breach.

A personal data breach may not be evident straightaway. However, there may be indicators of a personal data breach, system compromise, unauthorised activity, or signs of misuse. A personal data breach can happen in many ways, including:

- loss of a mobile device or hard copy file which contains personal data (e.g. leaving it on a train);
- theft of a mobile device or hard copy file which contains personal data (e.g. stolen from a vehicle or home);
- human error (e.g. a member of staff sending an email containing personal data to an unintended recipient, or accidentally altering or deleting personal data);
- cyber-attack (e.g. opening an attachment to an email from an unknown third party which contains ransomware or other malware);
- allowing unauthorised use/access (e.g. permitting an unauthorised third party to access secure areas of the office or our systems);
- unusual log-in and/or excessive system activity, in particular from any active user accounts;
- unusual remote access activity;
- the presence of any spoof wireless (Wi-Fi) networks visible or accessible from our working environment;
- equipment failure;
- hardware or software key-loggers found connected to or installed on our systems;
- unforeseen circumstances such as a fire or flood; or
- 'blagging' offences where information is obtained from us by a third party through deception.

If you are concerned about a potential personal data breach or have any reason to suspect a personal data breach has or is about to occur (for whatever reason), you should contact the HR department immediately by emailing hr@airnavigationsolutions.co.uk.

Personal data breach response plan

In the event of a personal data breach, we shall take quick action to minimise the impact of the breach and, in certain circumstances, if required, shall report the breach within 72 hours of it occurring.

Once a personal data breach or a potential personal data breach has been reported, the HR department will be responsible for responding to the data breach. In most cases this will involve:

- investigating the breach to determine the nature and cause of it, and the extent of the damage or harm that may result and if disciplinary action is appropriate;

- implementing the necessary steps to stop the breach from continuing or recurring, and limiting the harm to data subjects associated with the breach;

- assessing whether there is an obligation to notify other parties, in particular, the Information Commissioner's Office ("ICO") and the affected data subjects and, if so, making those notifications. If there is an obligation to make a notification to the ICO, this will normally need to be done within 72 hours of us becoming aware of the breach and therefore it is essential that any suspected or actual breaches are reported immediately;

- recording information about the personal data breach and the steps taken in response to it;

- If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken

PRIVACY NOTICE

This Privacy Notice provides information for staff about our reasons for processing personal data, how we use such data and the legal basis for processing.

What information do we collect?

For the purposes of this Privacy notice, personal information is any information about an identifiable individual, other than the person's business title or business contact information when used or disclosed for business communications. Personal information does not include anonymous or non-personal information (i.e. information that cannot be associated with or tracked back to a specific individual).

We process personal information about our:

- Current and future employees
- Job Applicants
- Customers and clients
- Suppliers and services providers
- Advisers, consultants and other professional experts
- Complainants and enquirers
- Training Delegates

Personal data we collect and process include but is not limited to:

- CVs and application forms
- Interview Notes
- Training Booking Forms
- Correspondence with or about you

The information we hold and process will be used for our management and administrative use only.

Such uses include but are not limited to

- Determining eligibility for initial employment
- Administering training bookings
- Dealing with customer enquires

We collect this information in a variety of ways. For example, data is collected through application forms and CVs, training booking forms, from forms completed by you at the start of or during your employment, from correspondence with you, through interviews, meetings or other assessments and through the website enquiry/contact from.

Data is stored in a range of different places, including in the organisation's HR management systems and in other IT systems (including the organisation's email and archiving systems).

Why does the organization process personal data?

We may need to process data to process your application or assess your suitability for employment, to enter into an employment contract or contract for services with you, to deliver training courses and to meet the obligations under contracts and terms and conditions..

In other cases, Air Navigation Solutions has a legitimate interest in processing personal data before, during and after the end of the contract. Processing data allows us to:

- operate and manage recruitment processes;
- complying with regulatory rules to which the Group may be subject;
- operating the e-mail and internet policy and other company policies and procedures;
- ensure effective general HR and business administration;
- conduct staff engagement surveys;
- provide references on request for current or former employees;
- deal with customer enquires and complaints;
- monitor, maintain and promote equality in the workplace, and;
- preserve the functionality and security of the IT systems.

Where we rely on legitimate interests as a reason for processing data, we have first assessed whether or not those interests are overridden by the rights and freedoms of our staff.

Who has access to data?

Your information may be shared internally within the business if access to the data is necessary for performance of their roles or specific task. In this instance, data shared would be limited to the information needed for the purposes of the performance of their role or specific task.

If we need to use third parties to process personal data on our behalf, we will require those third parties to provide us with sufficient guarantees that they have appropriate technical and organisational measures in place to comply with the GDPR and to ensure the protection of the rights of the data subjects. What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

Where necessary or required may share information with:

Third Party	What Information we may share?	For what purpose do we share this information?	Basis to Process Data
Nominated HR Management System	**Job Applicant Details (e.g. Name, Contact Details, gender, DOB, CV)**	**Provision and delivery of recruitment and applicant tracking system**	**Legitimate business interest**
Nominated Training Providers	**Name, Address, Telephone Number, Email Address, Dietary requirements**	**To enable booking and attendance of training courses**	**Contractual/Legal Requirement/ Legitimate business interest**
Nominated Law Firms	**Personal Details such as name and details relating to any dispute or claim**	**To mitigate risk and defend potential claims**	**Contractual/Legal Requirement**
Social Media Platforms	**Name, Photo**	**To promote the business and employer brand to the external market**	**Consent**
Nominated IT Management Systems	**Access to internal IT system**	**Provision and delivery of IT management system**	**Legitimate business interest**
Internal & External Auditors	**Dependant upon request received**	**To meet and evidence our audit requirements**	**Legitimate business interest/Legal Requirement**

The organisation may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

We do not currently transfer data outside of the EEA. If at any point in the future this changes, safeguards will be put in place in this regard and communicated to individuals.

For how long does the organization keep data?

Your personal data will not be kept for any longer than is necessary to fulfil the purpose(s) for which it was collected. For further information on data retention periods, please contact the HR department by emailing hr@airnavigationsolutions.co.uk

Your rights

If you believe that the organisation has not complied with your data protection rights, you should first contact the HR Department to discuss your concerns by emailing hr@airnavigationsolutions.co.uk. If you are not satisfied, you can make a complaint to the Information Commissioner's Office https://ico.org.uk