PRIVACY POLICY

Introduction

The General Data Protection Regulation (GDPR) is a new legal framework set up by the European Union in April 2016 to build upon existing data protection legislation. GDPR came into effect on 25th May 2018, and has introduced a range of fresh guidelines spelling out the rights of consumers and dictating how companies can store and share information.

As a hugely significant change to the global business landscape, it is critical that Airport Transport Centre embraces all aspects of GDPR to maintain full compliance.

Our obligations for GDPR compliance

Here at Airport Transport Centre, we fully appreciate and support the European Union's focus on expanding upon digital rights. As a company, we strongly believe in the need for greater business transparency and accountability concerning the collection and handling of personal data.

That is why Airport Transport Centre is a firm advocate of GDPR and its many implications. These include among many other aspects:

- The Right to Object to Processing
- The Right to Be Forgotten
- The Right to Data Portability
- The Right to Withdraw Consent

As part of our commitment to GDPR and the rights of our customers and clients, Airport Transport Centre vows to ensure our organisation considers and actions all necessary changes surrounding data processing, data storage and the disposal of personal data.

This includes a commitment to fully fulfil Breach Disclosure Requirements by notifying authorities and concerned individuals of any compromise within 72 hours. Moreover, as part of our GDPR strategy, Airport Transport Centre will complete impact assessments wherever possible, to identify and deliver the best service possible, as well as to extend our customers a guarantee that data is being kept secure.

Furthermore, we pledge to uphold the following key values and responsibilities:

Airport Transport Centre's strategic values and responsibilities

- We vow to demonstrate full responsibility and dutiful respect as a keeper of customer, client and employee data.
- We totally support GDPR and its requirements, and will do everything within our power to appropriately resource and fund any changes we must enforce to ensure Airport Transport Centre can meet its obligations.
- We promise to maintain ownership and transparency concerning data protection and privacy across all elements of our company.
- We pledge to create and maintain a purposeful data processing inventory documenting all data operations, including collection, processing and storage.
- We guarantee to extend every possible show of support to individuals intent on exercising their rights as outlined under GDPR legislation.
- We will conduct a regular review to assess the legality and purpose for the collection, processing and storage of personal data.
- We vow to act upon identified gaps and develop robust processes to maintain full GDPR compliance.
- We promise to clearly communicate the business purpose and legal grounds for any transfer of data – including transfer outside of the European Union.
- We will contact all partner organisations, contractors or other third parties to identify their own GDPR commitments, establish relevant contract terms and solidify GDPR compliance controls.

1. DATA SECURITY POLICY

Introduction

Here at Airport Transport Centre, we collect, process and store personal data for a range of business purposes. Data subjects include customers, suppliers, partners, employees, clients and other stakeholders and individuals.

Bearing in mind Airport Transport Centre's commitment to uphold the rights of the individual as enshrined in law, our data security policy is designed to protect all past, current and future employees, customers, or partners, from illegal or damaging activity conducted by others using their personal data.

Our data security policy outlines how Airport Transport Centre will endeavour to guard and protect all personal data. It also sets out to raise the awareness of staff members in relation to the ways in which GDPR impacts their use of individual's personal data.

This policy applies to all data processing activities involving Airport Transport Centre and includes activities or systems related to both internal business operations, as well as external relations and any third-party agreements.

Please note that Airport Transport Centre's data security policy applies to all employees, and this policy may be subject to review and amendment on a regular basis. For more information about this policy and its overall implementation, consult our Data Protection Officer.

This document is subject to regular review to ensure ongoing regulatory compliance.

Sensitive personal data

Under GDPR, sensitive personal data is defined as encompassing any of the following:

- Racial or ethnic origin
- Political opinion
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health-related information
- Sexual orientation

It is paramount that all sensitive personal data is kept under stringent control as part of the implementation of our data security policy.

Purposes of personal data

Airport Transport Centre uses personal data for a range of various purposes. These purposes may include:

- Financial
- Administrative
- Human resources
- Regulatory compliance
- Payroll
- Business development

Please note the above list is by no means exhaustive, and should merely be used as a reference point from which a working definition of purpose can be established.

Business purposes

Airport Transport Centre must carry out a range of functions and processes as part of our operational activity. Data kept in relation to these activities falls under the category of data for business purposes, which includes information of the following nature:

- Operational
- Compliance
- Policy adherence
- Human resources and personnel
- Marketing

The above list is by no means exhaustive, and should be used merely as a point of reference from which a working definition of business purposes can be established and further developed.

Fair processing

At Airport Transport Centre, there will be occasions when employees will need to process personal data; however, processing activities must always be carried out in a fair and lawful manner that is compatible with the rights of each corresponding individual. Consequently, we should avoid processing the personal data of any individual who has not provided us with explicit consent.

Our company must strive to obtain explicit consent at all costs, and we must clearly identify to the individual what data is being processed, why we need to use it and who will have access to their data. These factors must be identified and clearly reiterated to the individual at the point of request for consent.

It's worth noting there may be exceptional circumstances in which we are asked to process sensitive personal data without consent. An example of an exceptional circumstance could include legal obligations we may need to carry out to comply with health and safety regulations.

Airport Transport Centre endeavours to take all actions necessary to ensure that all personal data we obtain, process and store is accurate, relevant and adequate in relation to the reason in which we asked for that information. We should not hold excessive or irrelevant data on any individuals, and we will not process any personal data for a purpose unrelated to the purpose in which the relevant individual has consented to the processing of their data.

Our roles and responsibilities

Data security is a critical component of our business. It falls on everyone at Airport Transport Centre to take responsibility for data security, and all employees must familiarise themselves with our data security policy and do everything within their power to uphold that policy on a day-to-day basis.

Please note that Airport Transport Centre takes data protection incredibly seriously, and we expect all staff members to adhere to this data security policy. Any failure and refusal to comply with this policy could ultimately place our company at risk.

Bearing that in mind, personal non-compliance with this data security policy could lead to disciplinary action as they relate to ordinary personnel procedures. Please contact your line manager with any further questions concerning data protection at Airport Transport Centre.

As a staff member at Airport Transport Centre, you can expect to receive data protection training in line with our data security policy. All incoming employees will be provided training as an aspect of the wider staff induction process, and all staff members can anticipate the requirement to undergo additional training as a result of subsequent regulatory updates to GDPR or other relevant legislation as it relates to data security.

Data security will inevitably encompass a range of additional responsibilities for various roles within the company. These roles and their responsibilities include (but are not limited to):

Data Protection Officer

GDPR stipulates our company must appoint a Data Protection Officer. It is our Data Protection Officer's responsibility to:

- Organise data security training for all employees not specifically referenced within this data security policy.
- Review and analyse all existing data security protocols and processes on a regular basis.
- Be a point of contact for all employees, clients and stakeholders to answer questions about data protection and data security.
- Respond to internal or external queries from individuals wanting to know what data relating to them may have been obtained, processed or stored by our company.
- Conduct due diligence and submit approval in relation to any contractual agreement with a third party involving the processing or storage of data.
- Maintain constant contact with company directors, board members and stakeholders in relation to data security, company responsibilities and data risk management.

IT Manager

Information technology plays a crucial role in the way our company operates. Any processes relating to IT and the processing and storage of data must be carefully monitored, assessed and guided by an IT Manager.

It is the responsibility of Airport Transport Centre's IT Manager to:

Conduct due diligence and appropriate levels of research into any third-party service that our company may call upon to store or process any data.

Make sure that all company software, IT systems, equipment and services meet changing levels of data security standards.

Carry out regular checks, audits and scans to ensure security hardware and security software are fully functional and optimised to manage and mitigate data security risks.

Marketing Manager

A significant proportion of our marketing activities involve the collection, storage and processing of data. Consequently, our Marketing Manager must oversee the following responsibilities:

- Accept all queries relating to data security and data protection from leads, media outlets, clients or other individuals and oversee and deliver an adequate response.
- Work alongside Airport Transport Centre's Data Protection Officer to make sure that all of our marketing processes, campaigns and activities are compliant with all relevant data security and data protection laws – as well as our own company data security policy.
- Review, draft and approve any relevant data security statements that must accompany emails, other messages or applicable marketing collateral.

Our data security policies

Airport Transport Centre's takes data security extremely seriously, and we place the rights of the individual and regulatory adherence at the heart of everything we do as a company.

In light of our commitments, it is mandatory all staff members must observe and adhere to the following data security policies:

Data storage policy

- All information or data that is collected and processed is subject to all of the applicable requirements as outlined and documented within this policy. This includes information collected electronically, by paper, telephone or data collected through any other means.
- All data must be collected, stored and protected in a secure location appointed by Airport Transport Centre's for a retention period as predefined by corresponding legislature or company policy.
- Staff members are strictly forbidden to retain confidential information or personal data not relating to themselves on their personal devices. Exceptions to this policy include information that is needed for a purpose that is work-related, temporary and specified and approved by a relevant manager.
- Staff members should avoid downloading sensitive files or confidential information to local devices wherever possible. Information being necessarily processed for work purposes may be exempt from this policy.

- Employees must install and use software and systems that have been licensed and approved by the company on devices while carrying out the duties of their role. Downloading or using any software, app or system that is not preapproved by the company will require prior approval from the company's IT Manager.
- All mobile and portable devices used by staff members should be approved by the company's IT Manager and secured to prevent unauthorised access or breach. Personal devices could include a laptop, smartphone, tablet or any other handheld computing devices. This policy also applies to any shared cloud storage spaces.
- All internet access and online operations carried out by employees could be subject to monitoring and filtering in accordance with relevant legislation and company policy. This monitoring should be carried out only by the IT Manager or an authorised member of staff.
- Employees must adhere to all applicable elements of this policy when using personal devices to access company resources. Similarly, employees must observe and adhere to all applicable elements of this data security policy when using equipment provided by Airport Transport Centre's to access information externally.
- Employees are forbidden from using public access devices. This practice is allowed in some circumstances; however, prior and explicit approval from a line manager for regular public access must be obtained and recorded.
- Employees must use access tools provided to them by a client or partner of Airport Transport Centre's if access is granted to any third-party storage system or data storage facility.
- It is forbidden to send, forward or submit any of the information or data referred to within this data security policy to a third-party unless deemed essential to complete approved processes.
- If an employee needs to carry out an approved submission of data to any relevant third-party, that data must be made secure in accordance with company policy and any relevant third-party data protection protocols.

Please note that Airport Transport Centre's will carry out regular system audits to monitor and ensure ongoing compliance with this data security policy and all regulatory requirements as outlined under GDPR.

Data retention policy

While Airport Transport Centre must routinely collect and store data, we are committed to the rights of individuals. That's why we retain all information and personal data for no longer than we need to.

The necessary length of retention will often be decided on a case-for-case basis, bearing in mind the rationale and original purpose surrounding data collection and retention. Decisions of

this nature must be made in a way that is compatible with our existing data retention guidelines under GDPR.

For additional guidance, consult the following corresponding documents:

- Data retention and erasure policy document

International data transfer policy

Employees must observe a series of restrictions that apply towards the international transfer of data or personal information. Employees are not permitted to transfer personal information or data outside of the United Kingdom without having obtained explicit permission in the first instance from the company's Data Protection Officer.

Data encryption and anonymisation policy

Airport Transport Centre deploys encryption to secure and protect data that is stored on devices from unlawful processing or unauthorised access. Encryption is also used to protect information that is in transit.

We also use the anonymisation of personal data wherever deemed prudent to ensure the rights of the individual are fully protected and observed.

In line with these principles, we are committed to the use both encryption and anonymisation as a risk management tool alongside existing systems, to protect the company from accidental loss, as well as from the damage or destruction of data or personal information.

Activities that are prohibited

Unless otherwise noted or informed, employees are strictly forbidden from using company equipment, tools or systems for any purpose unrelated to their role responsibilities, excluding any previously mentioned exceptions. This policy also relates to any relevant systems, tools or equipment belonging to a company client or partner.

Bearing that in mind, the following activities should be deemed forbidden with no exceptions:

- Any unauthorised replication of copyrighted materials.
- The violation of individual rights by way of the unnecessary collection, storage and processing of personal data or information.
- The violation of rights of an individual or organisation protected under intellectual property law in any jurisdiction.
- The use of any programme, command or interface designed to interfere with a user or corresponding user session.
- The accessing of any data, user account or server for any purpose unrelated to the business function of an individual's company role.

- Issuing fraudulent product or service offers from a company account.
- The allowed sharing or use of employee login credentials or company systems by anyone apart from the named individual.
- The export of proprietary or confidential information as it relates to the company.
- The export of any software or data that is in breach of regulation or the company's data security policy.
- Knowingly causing a network disruption or security breach.
- An employee is not allowed to access data that is not intended for them by logging into a system or gaining access to a confidential or limited-access account. The only exception to this rule is if the employee is granted access as part of a specific company project.

Please note that any violation of this policy can lead to disciplinary action, alongside legal action where deemed prudent or necessary.

Reporting security issues

If you encounter any incidents or issues relating to the security or protection of information or data, you must report this immediately to company management. Management will subsequently take and record any action deemed necessary to prevent damage or loss in relation to a security threat.

If necessary, it is the responsibility of company management to report relevant incidents relating to a data breach or information security threat to regulators or the authorities. Under GDPR, it also falls upon management to contact the individuals involved in any breach or security threat.

2. INFORMATION AUDIT

Version: 1.1

Date:

Author: Khawar Siddiqui

Stored at:

Your data audit is a crucial tool in order to maintain ongoing GDPR compliance. We recommend you review this policy document every six months.

Name of data controller: Khawar Siddiqui

Date of audit completion: [DATE COMPLETED]

3. GENERAL DATA PROTECTION NOTICE

Introduction to your General Data Protection Notice

A General Data Protection Notice is a short document your company can use to set out the conditions under which you will capture or process the data of visitors to your website. This is ordinarily displayed in a clearly marked section of your company website, and it's important to bear in mind that the conditions you outline as part of your General Data Protection Notice do not include a request for marketing consent.

Your Data Protection Notice

Airport Transport Centre collects, processes and stores the information and personal data you submit to our website in relation for the execution of sales as booking. All processing activities shall be carried out in accordance with your individual rights as defined by the European Union's General Data Protection Regulation.

Please note that by submitting information about yourself through our website, you are agreeing for Airport Transport Centre to process and store that data. This data shall be stored only for the duration of the previously outlined purpose for collection. We never store or process your data longer than we need to, and we do not use your data for any purpose other than those you have agreed to.

The data you submit to our website will never be shared with or transferred to a third-party organisation. The following partners are exempt from this policy as they assist Airport Transport Centre in processing your personal data and delivering its services; Airport Transport Centre, drivers and operators.

You reserve the right to request Airport Transport Centre update your personal data at any time. You can also request information about your personal data, withdraw your consent for us to process your information or request a transfer or deletion of your data.

For more information about Airport Transport Centre and how we protect and secure your data, consult our Privacy Policy: https://www.airporttransportcentre.com/page/privacy-policy

Please tick this box to indicate you have read and consent to our Privacy Policy:

☐ Yes, I agree to Airport Transport Centre Privacy Policy

4. DATA CLASSIFICATION POLICY

1. Policy introduction

Here at Airport Transport Centre, we are committed to data security, the privacy of the individual and upholding all our compliance obligations under GDPR. We take our responsibilities seriously, and we recognise that the use of information assets and data form a crucial aspect of our business activity. That is why we've devised the following Data Classification Policy to outline the way in which we classify and use data.

- Our Data Classification Policy is designed to ensure that:
  Airport Transport Centre adheres to all necessary legal obligations
- We implement controls to maximise return on investment
  Airport Transport Centre maintains availability, confidentiality and integrity where necessary for all data
- Our company has the ability to chart data protection levels that protect both Airport Transport Centre as well as the individuals whose personal data we must collect, process or store
- We are able to avoid threats of disclosure and/or unauthorised access to data

2. Policy values

Data classification is a vital process our company must carry out to ensure the individuals who claim a legitimate right to access information we hold are able to do so. Our data classification process must also ensure our data and any other piece of information we hold is protected from any and all individuals or organisations that should not have access to that information.

Airport Transport Centre's Data Classification Policy identifies and elaborates upon the correct handling and classification processes our company must use, as per the regulatory requirements that we:

- Make data available to all those individuals who have a legitimate reason to access it
- Manage all data in line with its corresponding classification
- Maintain the integrity of all data
- Ensure all data our company holds is accurate, complete and consistent

3. Policy objectives

Airport Transport Centre's Data Classification Policy has been developed to meet the following objectives:

- To outline the duties and responsibilities of Airport Transport Centre employees that ensure data is kept safe and secure
- To establish a robust data classification process that is consistent and compliant with UK regulatory requirements
- To ensure data is sufficiently protected and encrypted so that unwarranted actions will not be taken against Airport Transport Centre in the event data is lost, damaged or accessed illegally
- To avoid and minimise reputational or operational damage to Airport Transport Centre, our stakeholders, clients, customers or partners associated with compromised data

4. Policy implementation

- To make sure our Data Classification Policy is effective, Airport Transport Centre will implement the following procedures:
- All users of data will be identified and provided access to data in which they have a legitimate need to access
- All data will be classified, managed and controlled in relation to its correct categorisation, as per the processes and requirements outlined within this policy
- Airport Transport Centre must ensure control mechanisms are created and implemented to protect data we collect, process or store
- All control mechanisms and classification protocols must be reviewed and amended as required by law on a regular basis
- Data users and data controllers must implement and maintain adequate levels of physical security as required, in relation to computer facilities or access terminals from which data can be viewed or accessed
- Airport Transport Centre must ensure that all data and relevant equipment is safely disposed of, as and when required

5. Obligations under GDPR (2018) and Data Protection Act 2018 (DPA)

Airport Transport Centre is committed to meet its regulatory obligations under GDPR and DPA. That is why we are committed to ensure that adequate and appropriate measures are taken to prevent the unauthorised access or illegal processing or storage of data. We are required to do everything we can, within reason, to protect the data we use and hold against destruction, accidental loss or damage.

6. Data classifications

Data that is sensitive in nature must be adequately protected at all times. To properly assign safeguards, all data that our company collects, processes or stores must be assigned one of the following classification categories:

- Public
- Open
- Confidential
- Strictly Confidential
- Secret

A vast amount of the data Airport Transport Centre uses will most likely be classed as being either 'Public' or 'Open' data. Any information relating to an individual or organisation that could identify them or is personal or private in nature must be assigned a category of either 'Confidential' or 'Strictly Confidential'.

This is to ensure Airport Transport Centre upholds its regulatory commitment to uphold the rights of individuals, as outlined under GDPR.

On rare occasions, Airport Transport Centre may wish to class data as 'Secret'. If an employee is unsure as to whether they should categorise a piece of data as being secret – or if they need assistance in classifying any other piece of data, they should consult a line manager. If no manager is available for consultation, data should default to a 'Confidential' classification.

7. Data classification types and handling procedures

To minimise discrepancies and ensure Airport Transport Centre does everything it can to uphold its regulatory commitments, the following working definitions should be associated with the aforementioned classification categories.

Public data

Public data is information or data that can be accessed by any external individual or organisation.

- Types of public data might include:
- Official contact data of relevant company employees
- News updates or press releases
- Company publications
- External-facing company policies or procedures

How to handle public data:

Public data should be formatted to allow for the most basic security measures. Examples might include converting a Word document into a PDF to avoid others editing it, as this could subsequently cause some form of reputational damage.

Open

Anyone is able to access this information.

Types of open data might include:

- Official contact data e.g. full name, primary email address and telephone number
- Authorised communications, such as blogs, news articles and industry updates
- Approved company policies, guidance and processes

How to handle open data:

Open data should be formatted to allow for the most basic security measures. Examples might include converting a Word document into a PDF to avoid others editing it, as this could subsequently cause some form of reputational damage.

Confidential data

Access to confidential data must be limited only to individuals who have been granted appropriate authorisation to view or process that information.

Alternatively, there may be occasions in which unauthorised individuals or stakeholders may need to be granted access to confidential data; however, this access must only be provided on a need-to-know basis.

Types of confidential data might include:

Someone's personal details or any information that could be used to identify them. Examples of identifiable or personal details include:

- Name
- Date of birth
- Address
- Telephone number
- Email address
- National Insurance number
- Race
- Religion
- Health details
- Political affiliations
- Trade union membership

- Criminal offences
- Employee contracts
- Non-Disclosure Agreements
- Unfinished or unapproved company documents
- Employee wage slips
- Death certificates
- PDR documentation

How to handle confidential data:

As and where required to handle confidential data, employees should exercise the following handling processes:

- Paper documents must be:
- In secure locked storage
- Transported in sealed envelopes only
- Transported by an approved third-party courier service
- Securely disposed of
- Electronic data must be:
- Encrypted
- Password-protected wherever possible
- Transportation must follow secure file transfer protocol
- Storage must be limited to secure file stores
- Securely disposed of

Strictly confidential data

A minimal number of authorised individuals, authorities or other stakeholders may be permitted access to data that has been classified as being ‘Strictly confidential’.

Types of strictly confidential data might include:

- Bank details
- Credit card information
- Financial information
- Server information
- Usernames or passwords
- Test data
- Medical records
- Disciplinary proceedings
- Patent information
- Network information

How to handle strictly confidential data:

As and where required to handle strictly confidential data, employees should exercise the following handling processes:

- Paper documents must be:
- In secure locked storage
- Transported in sealed envelopes only
- Transported by an approved third-party courier service
- Electronic data must be:
- Encrypted
- Password-protected wherever possible
- Tagged
- Transportation must follow secure file transfer protocol
- Storage must be limited to secure file stores

Secret data

Access to data that has been classed as 'Secret' or a request to access secret data is subject to the Official Secrets Act.

Various types of secret data may require different controls and circumstances. Bearing that in mind, individual protocols should be reviewed on a case-for-case basis in line with UK Government requirements. Government advice concerning the handling of secret data should be sought.

8. Data classification markings

Data classification markings need to be clearly visible at all times and must match the classification category in which that data has been assigned. Appropriate data classification identification markings should be included either at the top, bottom or centre of each document page.

9. Reclassifying data

There may be occasions in which data must be reclassified from one data category to another data category. The need for reclassification could depend upon a content change, or an alteration in terms of the data's intent, where it is stored or how it is being used. Before reclassifying data, a firm and justifiable rationale must be established. If in doubt, contact the Data Protection Officer or your line manager for guidance.

10. Sensitive data

It is the responsibility of the data owner or the data originator to define the category of data classification for a piece of data. Responsibility also rests with the data owner or originator to ensure that adequate protection has been afforded to that data in line with its relevant classification.

Any data that could or should be defined as being personal in nature must be afforded a higher level of protection and be treated as data that is sensitive. Personal data can be classed as information relating to an individual that could identify them. Aforementioned examples of sensitive personal data might include (among other pieces of data) a person's name, contact information, race, religion, political affiliations, sexual preference and so on.

Sensitive data must be identified and assessed on a case-for-case basis. In most cases, sensitive data will inherently be classed as confidential; thus, access and/or availability must be limited.

Sensitive data which is made available in the public domain can lead to reputational damage for private individuals or company employees. As a company we must ensure that sensitive data is given sufficient protection to protect individuals, company employees and the company itself.

11. Data storage and backup

Because data is such an integral aspect of our business, it is everyone's responsibility at Airport Transport Centre to do everything within their power to ensure that sensitive data is being collected, processed, backed up, stored and secured in line with company policy.

12. Data anonymisation

Prior to the sharing, transfer or disclosure of data, Airport Transport Centre and its employees must take all necessary steps to ensure that the anonymity of corresponding data subjects is protected and maintained in line with our regulatory commitments.

Necessary steps may include omitting or redacting (deleting) said personal identifiers within a piece of data. Audio visual data or verbally exchanged data recordings should be likewise edited.

13. Secure data disposal

Sensitive data that is no longer needed or has reached an 'end of life' classification as decided upon by the relevant authorised individuals must be disposed of in a secure fashion. Examples of disposing data as stored on paper would include shredding.

14. Data security response

If data is damaged or lost, it must be immediately reported to an appropriate line manager and company Data Protection Officer and logged as an incident requiring urgent response.

5. Controller Processing Activities Register

How should I use my Processing Activities Register?

Your company's Processing Activities Register should be used to document all of the ways in which you are handling and using data as a data controller.

Will I need to update my Processing Activities Register?

Yes. Your Processing Activities Register is a crucial tool in order to maintain ongoing GDPR compliance. We recommend you review this register every six months.

6. DATA RETENTION AND ERASURE POLICY

Data retention and erasure policy introduction

Our approach towards data retention

This policy is designed to ensure Airport Transport Centre does everything within its power to adequately protect, maintain and store data. This policy has also been developed to ensure that any data, documents or records that have no further use or value to Airport Transport Centre are disposed of in line with our regulatory obligations and relevant company policy.

Employees should consult our data retention and erasure policy, to develop an understanding of our company's obligations relating to the ways in which we retain data or electronic documents. These documents may include, but are not limited to:

- Emails
- Word Documents
- Spreadsheets
- PDF documents
- Web files
- Sound files
- Videos

Personal data must never be kept for longer than it is needed. Consequently, employees should utilise our company's data retention schedule as a guide to understanding Airport Transport Centre's general retention period time for various data categories that have been assigned based upon the purpose of the data. In line with our regulatory obligations, all data that is no

longer necessary should be deleted and all copies must be destroyed in line with our data erasure schedule.

Data retention schedule administration

This data retention schedule documents the maintenance, retention and disposal guidelines relating to any and all records our company holds. It must be reviewed and accordingly amended on a regular basis to ensure data storage and erasure processes are adhering to Airport Transport Centre's wider data retention policy approach.

There will be times when data may need to be retained longer than the pre-defined amount of time permitted. Circumstances in which our policy will need to be suspended may include, but are not limited to:

- Legal proceedings
- Regulatory investigations
- If criminal activity is suspected or alleged
- If relevant data concerns a company or organisation in receivership or liquidation
- If the relevant data is of historical importance to the owner or controller

In the event of legal proceedings, criminal activity or investigations, Airport Transport Centre and its employees must retain data that relates to the situation and could serve to aid the company's case or position, liability or amount involved. If such a situation may occur during the lifetime of this policy, Airport Transport Centre will inform all staff of the policy's suspension as it relates to said situation.

Data retention schedule

Airport Transport Centre has developed its data retention policy in line with the following data retention schedule:

Department	Function
1	Accounting and finance data
2	Contract data
3	Corporate records
4	Correspondence and internal memoranda
5	Personal data
6	Electronic data
7	Insurance data
8	Legal data
9	Miscellaneous data
10	Personnel records and data
11	Tax records and data

1. Accounting and finance data

Record	Retention period
Company financial statements and annual audit reports	Permanent
Annual audit records (including relevant documents)	7 years after audit completion
Company bank statements	7 years
Cancelled cheques	7 years
Employee expense reports	7 years
Interim company financial statements	7 years
Credit card records	2 years
Annual plans and company budgets	2 years

Any and all items that display customer bank details or credit card information must be kept under secure conditions when not in immediate use. This includes keeping printed records in a locked desk drawer or filing cabinet.

If Airport Transport Centre determines it is necessary to keep a document that displays customer financial details beyond a retention period of 2 years, all identifying details or financial information as it relates to any customer must be redacted or removed from the document in question.

2. Contract data

Record	Retention period
All company contracts	7 years after expiration or termination
All correspondence relating to contracts	7 years after expiration or termination

3. Corporate records

Record	Retention period
Corporate records	Permanent
Licenses and permits	Permanent

For the purpose of this schedule and corresponding policy, ‘corporate records’ should be defined to include anything relating to:

- Meeting minutes
- Signed minutes of the board

- Signed minutes of any committees
- Articles of incorporation
- Annual corporate reports

4. Correspondence and internal memoranda

The vast majority of correspondence and internal memoranda must be retained to match the period of time as the document or data to which they relate. Examples may include an email relating to a contract – in which case the email in question would be expected to be retained for a period of 7 years after the expiration of the corresponding contract.

Bearing this in mind, Airport Transport Centre recommends that all correspondence and internal memoranda as it relates to a company project be kept with said project as part of a project-wide file.

Company correspondence or internal memoranda unrelated to documents that have a defined retention period, should be securely destroyed at an earlier time depending upon which of the following two categories it corresponds:

Category 1

Category 1 correspondence or internal memoranda includes any and all data as it relates to routine processes. Category 1 correspondence and internal memoranda generally do not carry any significant consequences and should be disposed of with 2 years.

Examples of category 1 correspondence and internal memoranda may include (but are not limited to):

- Notes of appreciation or thanks
- Plans for meetings
- Forms or letters that do not require a follow up
- General enquiries that have been settled
- Chronological correspondence data
- Complaints requesting a specific action that have already been addressed and carry no further value
- Correspondence relating to inconsequential subject matter

All copies of internal office correspondence should be read and destroyed as per this policy unless that correspondence includes data or content that must be retained as part of a wider project.

Category 2

Category 2 correspondence or internal memoranda includes non-routine information or correspondence that is likely to have a consequential impact upon the company or its

employees. Category 2 correspondence and internal memoranda should be retained on a permanent basis.

5. Personal data

There will be times when Airport Transport Centre and its employees must retain and/or delete personal data in line with its legal obligations.

For the purposes of this data retention and erasure policy, 'personal data' can be defined as any identifying information as it relates to an individual. We never keep personal data for longer than is necessary for the purpose in which that data was collected. All personal data as defined within the following categories should be deleted based upon this retention and erasure schedule:

Record	Retention period
Data relating to customer devices	2 years after the account is closed
Data relating to use of our company website	2 years after the account is closed
Any data collected when registering with our website	2 years after the account is closed
Data collected and submitted as part of any profile creation processes	2 years after the account is closed
Data submitted for the purpose of subscribing to email marketing activities	Indefinitely (or until customer unsubscribes)
Data submitted as part of online service delivery	Indefinitely
Data relating to any subscriptions	2 years after the account is closed
Data posted in a public area on our company website	2 years after the post
Data contained in communications sent through the website	2 years after contact
Any other personal data	2 years after contact

Airport Transport Centre reserves the right to retain any and all documents (both electronic and print) containing personal data to the extent our company is required by law to do. We will also retain documents containing personal data if we have reason to believe said documents could be relevant to legal proceedings, or to establish and/or exercise our own legal rights.

Our company will organise backups of our database and all of the electronic data held within our company server(s). Backup activities should include all data that relates to current users or customers, alongside any document or dataset relating to one of the aforementioned reasons as outlined within this data retention and erasure policy. Airport Transport Centre does this to ensure that lost information can be retrieved within one year, as and where needed.

6. Electronic data

Emails

Most emails do not need to be kept. Emails that are inconsequential or unrelated to contracts or projects should subsequently be treated in line with the following policies:

- All emails should be deleted after 12 months. This includes both internal and external emails
- Airport Transport Centre will archive emails for six months after employees have deleted them. After this six-month period, archived emails will be destroyed
- Employees should never send emails containing confidential or proprietary data to external sources unless it has been approved by a relevant manager

Electronic documents

Electronic documents include, among other formats, both PDF document and files originating from Microsoft Office Suite or similar software.

Retention and erasure will depend upon the purpose of the electronic document, yet as a general rule of thumb employees can apply the following rules:

For PDF documents, the maximum period of retention should be 6 years. PDF documents that employees deem vital to their performance or role should be printed and/or stored in the relevant employee's workspace.

For text documents or other formatted files, the maximum period of retention should be 5 years. Text documents or other formatted files that employees deem vital to their performance or role should be printed and/or stored in the relevant employee's workspace.

Airport Transport Centre does not and will not automatically delete electronic documents or corresponding data beyond the time periods defined within this policy. It is the responsibility of our employees to ensure they are adhering to our policy guidelines.

7. Insurance data

Record	Retention period
Certificates	Permanent
Claims files	Permanent
Current insurance policies	Permanent
Expired insurance policies	Permanent

8. Legal data

Record	Retention period

Legal memoranda and legal opinions	7 years after resolution
Litigation data	1 year after expiration of appeals or time for filing appeals
Court orders	Permanent
Requests for a departure from Airport Transport Centre retention and erasure schedule	10 years
Register of members	Permanent
Director's meetings minutes	10 years

9. Miscellaneous Data

Record	Retention period
Reports from consultants	2 years
Documents containing content of historical value	Permanent
Original policy and procedures manuals	Current version with revision history
Copies of policy and procedures manuals	Retain current version only
Annual company reports	Permanent
Records of personal identification	5 years
Any work-related reportable accident, injury or death	3 years from incident
Immigration checks	2 years from termination of job

10. Personnel data

Record Type	Retention period
Job applications and/or related interview data concerning unsuccessful candidates	6 months
Employee personnel records	6 years after end of contract
Employment contracts	7 years after end of contract
Employment records correspondence with employment agencies	3 years from date of hiring
Job descriptions	3 years after superseded
Working time opt-out documentation	2 years
Financial details of employees	As long as necessary

11. Tax data

Airport Transport Centre keeps accounts and/or records to demonstrate and establish amounts of gross income, deductions, credits and other information. These records are crucial to maintaining our company's compliance of tax laws.

Associated records and documentation will include (but are not limited to) the following records and associated schedules:

Record	Retention period
Tax-exemption documentation	Permanent
Tax bills	7 years
Tax returns	Permanent
Tax receipts	Permanent
Tax statements	Permanent
Sales and/or use of tax records	7 years
Annual returns	Permanent
Payroll/wage records for unincorporated businesses	5 years after 31 Jan following the year of assessment
PAYE records	3 years from the end of the tax year to which they relate
Maternity records	3 years after the end of the tax year in which the maternity pay period ends

7.PRIVACY NOTICE AND CONSENT TEMPLATE

Privacy notice template

Your privacy notice is considered one of the most complex but crucial aspects of GDPR compliance. To help you to better understand your privacy notice and obligations under GDPR, we've broken this guidance document down into two sections:

A. General guidance
B. Privacy notice template

A. General guidance

Under GDPR, your company must provide explicit privacy information to any and all data subjects. These privacy statement stipulations are more specific and contain stronger specifications than what was previously expected of UK companies under the Data Protection Act 1998.

First and foremost, it's worth noting a privacy statement absolutely must be supplied by your company to any relevant individual at the point in time that they provide to you or submit their personal data. More important still, the statement that your company provides those individuals with must be:

- Concise
- Transparent
- Easily accessible
- Written in plain language
- Free of charge to access and read

Please note that additional rules are required if your privacy statement is designed for and/or directed at children.

To help you develop your privacy statement that complies with all of your GDPR obligations, we've compiled the following guidance sections.

Name and details of Data Controller

You must identify the name and contact details of the relevant data controller within your privacy statement. Here is an example of how your company may wish to outline these details:

Airport Transport Centre is the designated data controller for Airport Transport Centre and committed to upholding our commitments to protect the rights of individuals under legislation outlined within the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Name and details of data protection officer

You must identify the name and contact details of the relevant data protection officer within your privacy statement. Here is an example of how your company may wish to outline these details:

Airport Transport Centre has an appointed data protection officer Khawar Siddiqui to assist us in upholding our commitment to individual rights. Our data protection officer can be contacted both through our website https://www.airporttransportcentre.com/ , as well as by post Shelton Street, Covent Garden, WC2H 9JQ.

Description of the data being collected

Your company must explicitly describe the personal data you are collecting, storing or processing.

As a reminder, GDPR defines 'personal data' as being any type of information that includes an individual's:

- Name
- Location
- Any sort of identification number

- Any online identifiers
- Any physical identifiers
- Any attribute that could reveal their social identity

The aforementioned data types should also be applied to include any personal data surrounding employees, students or other stakeholders and clients.

This data includes:

- Name
- Date of birth
- Address
- Telephone number
- Email address
- Role
- Emergency contacts
- Passport or other identification

There are also special categories of personal data called sensitive personal data. This type of data generally includes information like:

- Race or ethnic origin
- Religion
- Sexual orientation
- Political affiliations
- Trade union affiliations
- Genetic or biometric data
- Health information

Sensitive data

If your company collects sensitive data, your privacy statement must explicitly outline what information you are collecting, where you are going to store it and how you are going to store it.

Here is an example of how privacy statement must address this responsibility:

“Airport Transport Centre must collect the following sensitive data about you so that we can deliver the executive service of transfer after booking:

- Travel itinerary, pay details, location, pay is process with our partner on drive who are fully complied under the PCI-DSS.

Airport Transport Centre needs your explicit consent for processing this sensitive data. We must request your signature for this consent.”

If your company does not collect sensitive data, you should state this within your privacy statement instead.

The age of consent for children

GDPR defines the point at which an individual is no longer considered a child is 16 years of age. That being said, GDPR empowers all EU member states to amend this age to either 13, 14 or 15 years old at their own discretion.

Bearing this in mind, data controllers are required to be aware of the age of consent in concerned member states. They are not permitted to seek consent from any individual under the specified age of consent within that individual member state.

If your company needs to obtain consent to collect, store or process the data of a child, you are permitted only to obtain consent to collect, store or process that data from an individual who holds parental responsibility for the concerned child. Your company must subsequently make reasonable efforts to verify the individual granting consent on the behalf of a child actually does hold parental responsibilities.

Privacy statements for children

If your company is offering services directly to a child, then relevant data controllers within your company must do everything they can to ensure that your company's privacy statements are written in a comprehensive and plain fashion that a child will be able to understand.

Online services being offered to children

The vast majority of consent requests your company will likely be required to collect, will be in relation to the provision of online services. Examples of online services could include provisions such as:

- Online stores
- Streaming services
- Social networking

The aforementioned rules in relation to the age of consent and corresponding privacy statements apply to most online services being offered. One exception to this is if your company is processing data relating to preventative or counselling services being offered directly to a child. Under such a circumstance, you do not need to seek consent from a parental figure.

Why data is processed

Your company must outline all of the reasons for processing data. Examples of processing reasons might include:

A. Financial administration
B. The provision of support services
C. The provision of information services
D. Account management
E. Research and analysis
F. The provision of operational information
G. Marketing
H. Safeguarding
I. Security
J. Crime prevention
K. To protect legitimate interests

You must state in your privacy policy any situations in which automatic decisions or actions are made within your company in relation to data.

Your company should also include a broad description of the ways in which you plan to use personal data, and the legal grounds supporting your ability to do so.

Furthermore, your privacy statement should also include a line similar to the following:

"Airport Transport Centre only uses personal data for the reasons in which we have collected. We will only ever use your personal data for another reason if we reasonably consider another purpose in which to use that data which is compatible with the original reason in which the data was collected.

If we are required to make such a decision, we will always notify you. We may also at times be required by law to process your personal data without your knowledge.

To find out more about the reasoning behind any decision Airport Transport Centre has made to process your data for a new purpose, get in touch."

If your company plans on using personal data for marketing purposes, you must explicitly say so. An example of how you may wish to convey this within your privacy statement could include:

"You may receive marketing communications from Airport Transport Centre if you have:

- Requested information from us
- Purchased goods or services from us
- Provided us with explicit consent for us to send you marketing communications
- Not opted out of receiving marketing communications

We will always ask for your consent before we share your personal data with any third-parties. You can ask us or any relevant third-parties to cease sending you marketing

communications at any time, by emailing us. You should send relevant requests to ksiddiqui@airporttransportcentre.com

Please note that if you opt out of receiving marketing communications from Airport Transport Centre, your personal data may still be retained as it relates to the provision or purchase of a product and/or service, warranty registration or other transactions."

Legal basis for processing personal data

To comply with your legal responsibilities under GDPR, your company must identify the lawful basis upon which you are processing an individual's personal data.

You must satisfy at least one condition under Article 6 of GDPR if you are processing personal data. If you are processing special category data, you must satisfy at least one condition under both Article 6 and Article 9.

Relevant conditions of these articles are outlined below:

Article 6: Personal Data	Article 9: Special Categories
Individual has given consent	Individual given explicit consent
Processing is required for delivery of contract	Processing is required to carry out obligations of controller or employment
Processing is required for legal compliance	Processing is required to protect vital interests of individual unable to provide consent
Processing is required to protect vital interests of the individual	Processing is required for legitimate activities by a foundation, association or any other non-profit with a political, philosophical, religious or trade union aim
Processing is required for a task that is in the public interest	Processing relates to personal data that has already been made publicly available by the individual
Processing is required for legitimate interests by controller or third party	Processing is required for reasons of substantial public interest
	Processing required to establish, exercise or defend against legal claims
	Processing is required for occupational medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of treatment or the management of health or social care systems
	Processing is required for reasons of public interest in public health
	Processing is required for achieving aims that are in the public interest or for scientific, historical or statistical purposes

If your company would like to utilise the legitimate interests basis, you must satisfy the following requirements:

- Your company must process data for the purposes of your legitimate interests or for those of a third-party to whom you disclose it
- Once the latter requirement has been met, the interests listed must be balanced against the rights of the concerned individual

Your company cannot rely on the legitimate interests basis in situations where the processing is unwarranted or has a prejudicial effect on an individual's rights or freedoms, as well as the legitimate interests of the individual. If your company's legitimate interests clash with those of the data subject, it is the legitimate interests of the data subject that will ordinarily be given precedence.

For every type of personal data you process, you should provide a description of the ways you intend to use this data, and the legal grounds for doing so. You should also explain the legitimate interests you have to process this data, where relevant. An example of holding this information is as follows:

Action	Data/Information type	Legal grounds for processing
Processing the delivery of products or services ordered, and actively managing the payments and debt recovery processes	(1) Personal identifiable information (2) Contact information (3) Financial information	(1) To complete the contractual agreement (2) Required for our legitimate interest of recovering any funds owed to us after the delivery of products or provision of services
Updating customers on any amendments to our terms and conditions or privacy policy	(1) Personal identifiable information (2) Contact information	(1) To complete the contractual agreement (2) Required to satisfy legal requirements
Registering a new customer	(1) Personal identifiable information (2) Contact information	(1) To complete the contractual agreement
Protecting our business and websites by performing website tests, applying security updates, assessing any cybersecurity threats and analysing our databases	(1) Personal identifiable information (2) Contact information (3) Website and Technical information	(1) Required to satisfy legal requirements (2) Required for our legitimate interest of protecting our websites and business from malicious usage, to prevent cybercrime, complete technical website audits and increase our network security
Emailing customers to request feedback or participation in a	(1) Personal identifiable information	(1) To complete the contractual agreement

prize draw	(2) Contact information (3) Product usage information (4) Marketing information	(2) Required to satisfy legal requirements (3) Required for our legitimate interest of studying how customers interact with our products and services offered, and how these can be further enhanced

The Data Recipients

Your company needs to explicitly state all of the recipients of data, as well as all of the recipients of categories of data. For the purposes of your company's privacy statement, a recipient can be actively defined as a natural or legal individual, public authority, agency or any other organisation to which personal data is submitted. This includes organisations that are third-parties, as well as subservient organisations within your company.

An example of the type of messaging you may wish to include in your privacy statement could run along the following lines:

"Airport Transport Centre may be required to share your personal data with carefully selected third-parties for the identified processing purposes. These third parties may include:

A. IT or system administration services providers
B. Professionals providing banking, legal, accounting, consultancy and/or insurance services.
C. Government regulators based in the United Kingdom and other relevant jurisdictions
D. HM Revenue & Customs
E. Stripe, drivers and sib contractors
F. Any existing or future third parties to which Airport Transport Centre may sell, transfer or merge aspects of our business or assets

All third parties to which we transfer data are required to respect your personal data, keep it secure and process it only for the specified purposes for which it has been collected. Third parties will only ever receive or process your data with our explicit permission."

Data transfers to countries outside the EU

If your company plans to transfer personal data to outside the EU, you must specify why that transfer is necessary, where the data will be transferred and to whom it will be transferred.

Data Retention Periods

Your company must state a specific retention period for which personal data will be stored. If it is not possible to share an explicit retention period, you must share the criteria that will be used to determine any retention period.

Automated decision-making processes

If your company will use data as part of an automated decision-making process, you must state the existence of those processes, the logic involved, and any consequences associated with those processes as they relate to personal data.

Where/how data is collected

In instances in which your company has not obtained personal data from the data subject directly, you must cite who this data was obtained from.

Individual rights

Your company has an obligation to inform individuals about their rights under GDPR. This includes their right to access and port data, their right to rectify incorrect data, restrict use, object to processing or withdraw consent.

An example of how your company may wish to explain this within your own privacy statement could run as follows:

“Airport Transport Centre respects your rights. We fully observe your right to access your personal data, to object to the processing of personal data, or to erase, restrict, rectify or port your personal data. Relevant requests can be made to Khawar Siddiqui at Shelton Street, Covent Garden, WC2H 9JQ.

Visit us online at https://www.airporttransportcentre.com/ for further details relating to your individual rights.”

Information security

If you collect, store or process personal data, you must explain the security measures your company has in place to protect that data.

An example of how your company may wish to explain this within your own privacy statement could run as follows:

“Airport Transport Centre has implemented a series of security measures to make sure that your personal data is protected from accidental loss, unauthorised access, alteration or disclosure. Airport Transport Centre limits access to your data only to those employees, agents, contractors or other third parties with a legitimate reason to access that information. Those individuals or organisations will only ever process or access your personal data upon our explicit instructions. They are subject to a duty of confidentiality.”

Complaints

You must provide individuals with a complaints procedure if they are not content with the way in which their personal data has been collected, stored or processed.

An example of how your company may wish to explain this within your own privacy statement could run as follows:

"If you are not happy with how your personal data has been processed, you should contact Khawar Siddiqui in the first instance by using the contact details listed above. If Khawar Siddiqui is unable to satisfy your concerns, you have the right to apply to the Information Commissioner's Office for a resolution.

You can contact the Information Commissioner's Office at the following address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
www.ico.org.uk "

B. Privacy notice template

Please note the following privacy notice is a template only. Particular sections of this template may or may not apply to your business, and you may be required to add new sections, statements or information based upon your own unique company needs or data requirements.

Frequently asked questions

Who is using my data?	Airport Transport Centre
What is my data being used for?	Airport Transport Centre stores and processes data to help us maintain your account, process and store transaction details, offer customer support, send system updates and send offer details.
What will happen to my data?	Airport Transport Centre may use your data to send you information, updates and offers we think you'll be interested in.
What data will be kept and stored?	Airport Transport Centre stores registration details, transaction details, usage information and any information about your web preferences on our website.

What data will be shared with others?	We only share your data with regulators or government bodies if requested.
How long will my data be kept for?	Airport Transport Centre will store your data for a period of 6 months after your last attempted login. After this period, your account will be deleted. You can request your account to be delete at any time.
Who will be able to access my data?	Airport Transport Centre will never sell or share your data to any third-party, unless you grant us your explicit permission to do so.
How will my data be kept and made secure?	Airport Transport Centre stores your data on secure servers that are based in the UK. Data is processed in the UK, and we use standard industry security protocols.

Privacy Notice

Airport Transport Centre takes your privacy seriously. That is why we will only use your personal information to provide you with the products and services you have requested, as well as to administer your account. We will not sell or share your information with third-parties you grant us explicit permission to do so, and we will never use your personal data for any reason other than the reasons described within this policy.

About our privacy policy

Our privacy policy outlines your relationship with our company and explains in detail how we use the information that you provide us with.

About Airport Transport Centre

Airport Transport Centre is the trading name of Airport Transport Centre which is registered in England and registered with the UK's Information Commissioner's Office under the Data Protection Act 2018. Our data controller is Khawar Siddiqui, and we encourage you to get in touch with any questions you may have about Airport Transport Centre.

You can reach us by:

- Post: Shelton Street, Covent Garden, WC2H 9JQ
- Telephone: +44 203 198 7000
- Email: ksiddiqui@airporttransportcentre.com
- Website: https://www.airporttransportcentre.com/

Changing your preferences

If you'd like to change your web, contact or marketing preferences, you can do so at any time. Simply contact us at ksiddiqui@airporttransportcentre.com to request the necessary amendments.

How we do business

Airport Transport Centre is committed to upholding and maintaining your personal rights. We operate our business in-line with the European Union's General Data Protection Regulation and observe your rights to change or withdraw your opt-in options at any time. As part of our ongoing commitment to uphold your rights, Airport Transport Centre will also extend advice on how you can issue formal complaints to relevant authorities, such as the Information Commissioner's Office.

Sensitive data

Airport Transport Centre does not collect any sensitive data about you. Sensitive data refers to (but is not limited to) information about your race or ethnic background, religious or political affiliations, trade union affiliations, sexual orientation, criminal background or health background.

Who our privacy policy applies to

This privacy policy has been developed to inform users of Airport Transport Centre how we use their data. Airport Transport Centre is an executive transfer service, and we need to process the data of individuals to offer our products and/or services. Bearing that in mind, our privacy policy applies to any and all individuals registered with us as a user, customer, administrator or in any other capacity.

What information this policy applies to

There is a lawful basis for processing your data, and this section of our privacy policy outlines how this applies to the personal information you provide us with or allow us to collect.

The information this policy applies to includes information that you:

- Provide as part of any registration process
- Provide as part of any campaign creation activity
- Provide in the form of numerical data, metadata or communications
- Give us as part of our ongoing relationship

This policy also applies to information that we:

- Collect relating to how you interact with our website
- Must process to complete purchases and other transactions

Consent

Please note that when you submit personal data on our website, you are giving Airport Transport Centre your explicit consent that we can use that data in line with our privacy policy.

Opting-out

After giving Airport Transport Centre your consent, you are free to amend your consent or withdraw your consent at any time. You have the right to object to the processing of your data. To opt-out, change your preferences or revoke your consent, simply contact us by emailing ksiddiqui@airporttransportcentre.com

Data processing and storage

Airport Transport Centre collects and stores data in the UK. We will store your data for a period of 6 months after your last recorded login attempt unless otherwise noted and explicitly stated.

Airport Transport Centre stores data relating to transactions, payments and orders for a period of up to seven years. This period may be extended under certain circumstances as part of our ongoing commitment to comply with UK and international law.

We use carefully selected and recognised third-parties to help us take payments, provide commerce services and manage company accounts. Some of these third-parties may operate outside the European Union.

Airport Transport Centre may process your data based on more than one legal ground.

Circumstances under which we may be required to process your data under more than one legal ground may include:

Reason	Data type	Legal basis
Customer registration	Identity and contact information	To carry out a contract we've made with you
Processing and/or delivering your order	Identity, contact information, financial information, financial and transactional data	To carry out a contract we've made with you and to exercise our legitimate interests to recover debts owed
To manage our customer relationship with you	Identity, contact information, marketing and communications preferences	To carry out a contract we've made with you, to comply with legal obligations and to exercise our legitimate interests to keep our records updated

Marketing and communications

Airport Transport Centre may send you marketing communications if you have given us your contact details and opted-in to marketing communications.

You can opt-out of these marketing communications and manage your preferences at any time.

Our company obligations

As a data controller, Airport Transport Centre is legally responsible for the data you provide us with. In honouring that responsibility, we pledge to uphold our commitments under GDPR and the Data Protection Act 2018.

We will only ever use your data:

- In ways that are both fair and legal
- As described within this policy
- In ways that are necessary for the purposes described

In addition, Airport Transport Centre processes the personal data you submit to us or we collect as a data processor. As part of this role, Airport Transport Centre takes all necessary precautions to secure the personal data we collect, process and store.

We may occasionally use the data you provide us with for marketing, relationship management or account management activities. These activities are designed to ensure you have adequate information about other products and/or services we offer, that we have reason to believe you may be interested in. You have the right to opt-out of these activities at any time.

Third-Parties

Airport Transport Centre never shares your personal data with third-parties unless those parties have been explicitly mentioned within our privacy statement.

Our security

As part of our ongoing commitment to GDPR, Airport Transport Centre will report any security breaches or attempted breaches to the relevant authorities within 24 hours. We will subsequently contact all those affected by the breach within 72 hours of its occurrence.

Legitimate interests

As part of the Data Protection Act 2018, Airport Transport Centre observes the right to share selected information with third-parties that use data for non-marketing purposes. This could include (but is not limited to) organisations that provide credit assessments, identification services and fraud prevention activities.

Contact us

Airport Transport Centre is committed to upholding your rights. If you have any questions, comments or concerns about this privacy policy or wish to exercise your rights in relation to your personal data, please contact Khawar Siddiqui at Airport Transport Centre.

We will process any request within 20 days. Subject Access Requests are normally performed free of charge, but we may need to charge individuals for excessive or unreasonable data requests.

8. DUE DILIGENCE CHECKLIST

Introduction to your due diligence checklist

The following template offers a comprehensive checklist of the criteria you must assess to ensure your company's suppliers are GDPR compliant. Any additional questions or need for clarification you may have for a particular supplier should be added to the bottom of this checklist as and when required.

Name of supplier	
Named supplier representative	
Contact address of supplier	
Review date	
Scheduled date for next review	
Name of company representative conducting check	

Contract details information	
Are GDPR responsibilities defined within Airport Transport Centre contract with the supplier?	
Does the supplier take full liability in the event of a security breach?	
Does the supplier take partial liability in the event of a security breach?	
Has Airport Transport Centre reviewed all contracts with the supplier?	
Has the supplier defined GDPR responsibilities in their employment contracts?	
System security information	
Does the supplier take responsibility for data security?	
Has the supplier documented its system coding and design?	
Does the supplier carry out security testing on a regular basis?	
Has the supplier taken all of the necessary steps to protect their systems?	
Does the supplier encrypt data that is either 'at rest' or 'in flight'? (Note: this should include data exchanges such as email interaction or APIs.)	

Data subjects information	
Which individuals within the supplier's business hierarchy have access to various data subjects?	
What data can those authorised individuals access?	

Why do those authorised individuals have access to that data?
Does the supplier use a ‘privacy by design’ approach in securing subject data?
What type of access and what rights to access does this supplier give to relevant data subjects?

Data security information	
Is the supplier capable of fulfilling a subject access request?	
What is the supplier’s process for fulfilling a subject access request? (If applicable)	
Does the supplier log changes to data?	
Does the supplier report on logged changes to data?	
Does the supplier implement right to be forgotten requests?	
Does the supplier log right to be forgotten requests?	
Does the supplier offer data portability in a usable format?	

Standards information	
Does the supplier in question observe ISO9001?	
Does the supplier in question observe ISO27001?	
Does the supplier in question have a Cyber Essentials certificate?	
Does the supplier in question have C-base?	
Is the supplier in question a member of the ‘Investors in People’ scheme?	

Financial information	
Has a satisfactory Companies House review of the supplier been successfully completed?	
Has a satisfactory FCA/MOJ/ASA/ICO review of the supplier been successfully completed?	
Has the supplier in question been administered a credit check?	
Has the supplier in question passed a credit check?	
Will the supplier indemnify Airport Transport Centre in the event of a security breach?	

Insurance information	
Does the supplier in question have cyber insurance coverage in place?	
Does the supplier’s insurance coverage extend to data protection?	
Does the supplier’s insurance coverage extend to breach protection?	
Does my supplier carry professional indemnity insurance? (yes/no)	

Privacy information	
Does the supplier in question restrict access to data to authorised personnel only?	
Does the supplier encrypt data?	
Has a security review been conducted of Airport Transport Centre's supplier systems?	
Does the supplier ever use Open Source platforms?	
Does the supplier in question audit the use of third-party plug-ins, themes or apps surrounding the use of Open Source platforms? (If applicable)	

Data recovery information	
Does the supplier have a release management policy in place?	
Does the supplier have a clearly outlined and clearly well-defined data recovery policy?	
Does that data recovery policy include relevant protocols to ensure that no breaches occur if and when data must be restored?	
Does the supplier have a data backup policy in place in the event of a system failure?	
What does the supplier's data backup policy procedure entail?	
Does the supplier in question have a disaster recovery plan in place?	
What does the supplier's disaster recovery plan entail?	

Data breach information	
In the event of a data breach, does the supplier have a recording pathway?	
What is the process by which Airport Transport Centre will be informed of a data breach?	
What is the process by which data subjects will be informed of a data breach?	
What is the process by which relevant third parties will be informed of a data breach?	

Audit and reporting information	
Does the supplier in question offer any sort of audit of their services?	
Is the supplier able to demonstrate their GDPR compliance?	
How regularly does the supplier conduct reviews of the compliance?	
Is the supplier able to provide an audit report demonstrating GDPR compliance?	

GDPR compliance information	
Based on the aforementioned checklist items, is the supplier in question GDPR compliant?	
Has the supplier in question audited their own suppliers or vendors?	
Does the supplier have a risk management process in place?	
Does the supplier have an appointed Data Protection Officer?	

Supplier due diligence checklist results – Fail/Pass/Additional information required

Additional information required

9. SUBJECT ACCESS REQUEST FORM

A. Subject access request process

Airport Transport Centre is committed to upholding the rights of individuals as defined under GDPR. This is why we observe the right of individuals to request any data that we may hold on them as part of a recorded subject access request.

We are committed to performing subject access requests in a timely and accurate manner. For guidance purposes, subject access requests should adhere to the following six steps:

- Receive and record the subject access request
- Verify the identity of the individual making the request
- Process the subject access request
- Verify response
- Respond to the subject with the relevant information
- Record the request and following interactions

B. Subject access request form

Please complete this form if you'd like Airport Transport Centre to supply you with a copy of any data relating to you that we may hold.

Airport Transport Centre observes your right and entitlement to receive this information under the European Union's General Data Protection Regulation and the Data Protection Act 2018.

As part of your subject access request, Airport Transport Centre will also supply you with information about any processing activity that has taken place involving your personal data, as well as the period of retention that has been applied to the data in question.

After receiving this request, Airport Transport Centre will provide you with a confirmation of receipt, as well as a confirmation of receipt concerning any additional information we may ask you for to process your request.

Upon your examination of this data, please note that you have the right to request corrections to be made, restrict use or tell us to delete your information.

Please note that the information you provide us with as part of this request form will be used solely to identify the data you are requesting and to respond to your request. You do not need to complete all fields of this form if you do not wish to do so, but completion will enable us to better facilitate your request.

1. Your contact details

First name	
Last name	

Address	
Telephone	
Email	

2. Are you requesting information about yourself?

Airport Transport Centre is committed to protecting your data, and so to ensure that we are releasing your personal data to the right person, we will need you to supply us with proof of identity and address.

To verify your identity, please send us a scan or photocopy of one item from both of the categories below:

- Proof of your identity
  - Passport
  - Driving licence
  - National identity card
  - Birth certificate
- Proof of your address
  - Bank statement
  - Utility bill
  - Credit card statement (must be under three months old)
  - Current driving licence
  - Current TV licence
  - Local authority tax bill
  - HMRC tax document (must be under one year old)

Please do not send original copies of documentation.

If you are unable to provide us with sufficient evidence to verify your identity Airport Transport Centre reserves the right to refuse your subject access request.

3. Are you requesting information on behalf of someone else?

If you are requesting data on the behalf of the individual that data relates to, you must include the following alongside your completed subject access request form:

- Written consent from the data subject giving you authority to request this information
- Proof of the data subject's identity
- Proof of your identity

To verify your identity and the identity of the data subject, please send us a scan or photocopy of one item from both of the categories below:

- Proof of your identity
- Passport
- Driving licence
- National identity card
- Birth certificate
- Proof of your address
- Bank statement
- Utility bill
- Credit card statement (must be under three months old)
- Current driving licence
- Current TV licence
- Local authority tax bill
- HMRC tax document (must be under one year old)

Please do not send original copies of documentation.

If you are unable to provide us with sufficient evidence to verify your identity, Airport Transport Centre reserves the right to refuse your subject access request.

First name	
Last name	
Address	
Telephone	
Email	

C. What information are you requesting?

In the box below, please tell us the information you would like to receive, alongside any information or details you think may assist us in identifying the data in question to process your request.

Please specify if you would like to receive any details relating to why Airport Transport Centre is processing your data, who has access to that data and how we were supplied that data.

Please note there may be situations in which disclosure of data or information could adversely affect the rights of others. If we believe disclosure of data to you is not compatible with our duty to uphold the individual rights of others, we will explain this to you, outlining our reasoning.

Airport Transport Centre will strive to process and complete your subject data access request in a fashion that is satisfactory to all parties; however, there may be times when we cannot provide you with copies of the data you have requested if it would take disproportionate effort. We reserve this right under the Data Protection Act 2018.

Please note that while Airport Transport Centre strives to carry out and complete subject access requests to all individuals free of charge, we reserve the right under Article 12 of the General Data Protection Regulation to charge a nominal fee or refuse a request that is considered manifestly unfounded or excessive.

D. Your declaration

Please read and sign the following declaration for us to process your subject access request.

I confirm that I have read the terms of this subject access request form and understand those terms. I hereby certify the information I have provided on this form is true and accurate. I understand it is necessary to verify my identity and/or the identity of the aforementioned data subject to process this request. I understand I may be asked to submit more information to facilitate this request.

Signature: _____

Date: _____

C. Subject access request response

Subject line: Subject access request: reference *|REFERENCE NUMBER|*

Dear *|NAME OF INDIVIDUAL|*

Thank you for your request dated *|DATE REQUEST WAS MADE|* concerning *|DATA SUBJECT|*. We have processed your request, and are pleased to enclose the requested information.

|INFORMATION REQUESTED|

We hope you find provision of this information satisfactory. Please do not hesitate to contact us with further queries.

Best wishes,

Airport Transport Centre and Khawar Siddiqui

D. Subject access request log

Airport Transport Centre records all subject access requests. Please use the table provided to document all requests and their corresponding outcomes.

Subject access request number	Date request received	Data subject identity confirmed	Request response verified	Request response submitted	Total number of days to request completion

10. DATA BREACH POLICY, LETTER AND REPORTING

Data breach policy, letter and reporting

Here at Airport Transport Centre, we take privacy seriously. That is why we take every possible precaution to protect personal data, and actively work to avoid any data protection breaches which could compromise our data security, or the personal rights of our clients, customers, stakeholders or anyone else associated with our company.

To mitigate the risk that any such data compromise could pose, we have developed the following data breach policy. It is an integral part of our compliance responsibilities under the General Data Protection Regulation and Data Protection Act 2018, and is designed to develop clear lines of responsibility and processes that must be followed to adequately mitigate and manage data breach and security incidents.

What does this policy cover?

The scope of this data breach policy encompasses all personal and sensitive data our company holds. This data breach policy applies to everyone at our company – including employees, temporary or casual staff, consultants, suppliers, contractors, freelance workers or other data processors who are storing or processing data on the behalf of our company.

What is the purpose of this policy?

The purpose of this data breach policy is to contain all data breaches and to minimise the risks associated with any breaches. It also outlines the actions that should be taken in the event of a breach to ensure data is secure and to prevent further breaches.

About data breaches

A data breach is defined as any incident, event or action that has the potential to compromise the availability of data, the integrity of data, confidentiality or our company's data systems. This includes incidents or events that happen by accident or deliberately. Both confirmed and suspected incidents may qualify as a data breach.

For the purposes of this data breach policy, an incident may include (but is not limited to) any of the following:

- Unauthorised use or accessing of data
- Unauthorised modification of data
- Loss of personal or sensitive data
- Theft of personal or sensitive data
- Loss or theft of equipment on which data has been stored
- Individual error
- Any attempts to gain access to data or our company IT systems (both successful or failed)
- Defacement of web property
- Physical incidents, like a fire, which could compromise IT systems

How to report a data breach

All employees who access, manage or use data in any way are responsible for reporting a data breach or any other type of security incident. This report should be made immediately to the employee's line manager, using the data breach reporting form.

This report must include full details of the incident or breach, when it occurred, who the data relates to and how. It must also include details about the individual reporting the incident.

If a data breach or a data security incident occurs outside of normal company hours, or a data breach or data security incident is discovered outside of normal company hours, it must be reported as soon as possible.

Any violation of this data breach policy could result in disciplinary action procedures taking place for company employees.

Data breach containment and data recovery

All necessary steps must be immediately carried out to minimise the effects of any data security breach or data security incident. This process of containment should begin with an initial assessment designed to establish the severity of the incident. The initial assessment should also include analysing whether there is any way to recover the lost data, and mitigate further risks associated with the incident.

Your initial assessment should include the following information:

- The data involved
- Whether the data involved is sensitive in nature
- The individuals affected
- The security measures that are in place to protect the data
- What has happened to the data
- Whether the data involved could be used in an illegal or otherwise inappropriate way
- Any perceived wider consequences associated with the breach or incident

Data breach notification

Airport Transport Centre will determine which individuals must be notified in the event of a data breach or data security incident. Each incident must be assessed on a case-by-case basis. In every instance, the following considerations will be made:

- Any contractual notification requirements
- Any legal notification requirements
- How many people are affected
- What consequences may occur as a result of the data breach or data security incident
- Whether notification of a breach or incident would help the individual to mitigate risks associated with the incident
- Whether notification could assist the company in meeting its legal obligations under GDPR and Data Protection Act 2018
- Whether notifying an individual could prevent the unauthorised or illegal use of data
- Whether Airport Transport Centre must notify the Information Commissioner's Office

All data breaches and data security incidents, both suspected and verified, must be recorded, to assist in further analysis and to help prevent further breaches.

The danger of notifying too many individuals

There will be data security incidents in which a large number of individuals will need to be notified. However, there will be other incidents in which notifying a large number of individuals may have the potential to cause disproportionate enquiries.

Whenever we notify an individual whose personal data has been affected by an incident or breach, that notification must include a description of when the breach occurred, how the

breach occurred and what data was involved. Notifications must also include explicit guidance concerning what said individual can do to protect themselves. We should also outline to concerned individuals what steps our company has already taken to mitigate risks.

Data breach evaluation and response

After the data breach or data security incident has been contained by carrying out all necessary measures, Airport Transport Centre will conduct an extensive review detailing:

- The cause(s) of the breach
- The effectiveness of any responses
- Whether changes to existing IT systems, company procedures or policies must be implemented

All existing protocols must be reviewed to analyse their adequacy. Any necessary amendments to protocols must be identified and carried out as soon as possible.

Data breach report form

Please complete this form in the event of a data breach or data security incident:

To be completed by employee	
Date of incident	
Date incident was discovered	
Name of the individual reporting incident	
Contact details of the individual reporting incident	
Where the incident occurred	
Description of the incident	
Number of data subjects affected by incident	
Personal data placed at risk by incident	
Description of any actions taken at the point of discovery	

To be completed by the Data Protection Officer or Airport Transport Centre management	
Name of individual receiving report	Khawar Siddiqui
Date report received	
Name of individual the report was forwarded to for action	
Date the report was forwarded for action	

Data breach letter

Dear [Customer Title and Surname],

We regret to inform you that Airport Transport Centre has discovered a breach in our processing system that has exposed your personal data to unauthorised use by external parties. We have notified the Information Commissioner's Office (ICO) and relevant law enforcement agency about this incident and will work with cyber security experts and legal counsel where needed to minimise any further risk posed to you by this incident.

About the incident

We appreciate you're going to have questions and concerns relating to this data incident, and we will do our best to explain the situation, what happened and why.

Airport Transport Centre has conducted an investigation and we believe the following events led to the data security incident in question:

- [List timeline of events here]
- *DETAILS*

About the data involved

We believe the following personal information about you may have been unlawfully accessed or affected by this data security incident.

What this means for you

Following the investigation Airport Transport Centre has carried out as part of this data security incident, and bearing in mind the type of information or data relating to the incident, we believe you may experience the following consequences as a result of this incident.

As a result, we would recommend you take the following actions as soon as possible to further protect yourself from additional risks associated with this incident.

What will we do to prevent this from happening in the future?

Here at Airport Transport Centre, your privacy is one of our top concerns. We do everything we can to ensure your personal data is made secure and your individual rights are preserved and upheld at all times. On this occasion we have fallen short, and we wholeheartedly and unreservedly apologise.

To ensure that data security incidents like this do not occur in the future, Airport Transport Centre is already taking the following steps to eliminate future risk and minimise the impact such threats could pose to you in the future.

What happens next?

We will not send you further email updates relating to this incident unless you explicitly request information. Any further emails you may receive about this security incident should be treated as suspicious, and we would encourage you to verify the authenticity of any further correspondence relating to this incident by contacting our Data Protection Officer, Khawar Siddiqui at ksiddiqui@airporttransportcentre.com

We will publish future updates relating to this data security incident on our website, which you can access here: https://www.airporttransportcentre.com/

Once again, we would like to take this opportunity to apologise for this breach of security. We promise to do everything within our power to make sure this never happens again.

If have additional questions about this incident or your individual rights, please contact our Data Protection Officer, Khawar Siddiqui at ksiddiqui@airporttransportcentre.com

Data breach reporting

Please complete all fields of this form.

Breach identification number	Date logged	Impact on Data Subject	Breach confined	ICO notified of the Breach	Data subjects notified

11.LAWFUL BASIS FOR DATA PROCESSING

GDPR, lawful basis and legitimate interests

Under GDPR legislation, companies wishing to process data are permitted to do so if they can justify the relevant processing activities under at least one of the following six categories of lawful basis:

- The data subject has given your company consent to process their data for a specific reason
- Processing data is necessary to carry out the delivery of a contract with the data subject
- Processing data is necessary to protect the vital interests of the data subject or another individual
- Processing data is necessary for the delivery of a task that is being carried out in the public interest
- Processing data is required to meet your company's compliance with legal obligations
- Processing is required for a legitimate interest being pursued by your company or a relevant third-party (note this category does not apply if your company's legitimate interests clash with the individual rights of the data subject)

There is no established hierarchy in terms of the lawful bases you can apply as your reason for processing data. Different bases can be applied to different activities, and may depend upon the types of personal data being processed at any given time. Consent is often considered the most explicit and strongest form of legal basis.

It's also worth noting that "legitimate interests" is not a phrase defined by the European Union's GDPR legislation, and so is subject to limited interpretation.

For the purpose of GDPR compliance, the legitimate interests of your company or data controllers operating on behalf of your company generally provides a legal basis for processing data. This is the most common form of lawful basis; however, this category of lawful basis cannot be applied in any situation in which the processing activity in question could impair an individual's rights or freedoms.

If your company decides to use legitimate interest to support the lawful basis of any processing activity, you must carefully assess whether the data subject would reasonably expect the processing activity for which you have collected data to take place. If the data subject would not reasonably expect further data processing to take place that is supplemental to the rationale originally applied, it could negate your company's ability to claim legitimate interests as a reason for processing data

Please note there may be situations in which the legitimate interests of your company or data controller may overlap with other bases for lawful processing. For example, under GDPR, it is acknowledged within the legislation that data controllers can apply a legitimate interest for any processing activity required to ensure the security of information systems, or as part of a task that is being carried out in the public interest.

Likewise, any data processing activity relating to public health can be lawfully carried out both in the legitimate interest of a data controller or company, but also to protect the vital interests of the data subject in question.

Finally, you must bear in mind that regardless of the legal basis you choose to support each data processing activity, that basis can be removed if the data subject decides to object to processing.

Your company must consider what tools are in place to allow individuals to submit their objections. For example, the right to object to direct marketing activities such as email communications could be extended through inclusion of an unsubscribe link or online communications preferences centre.

Your company should always assess the impact of a potential objection prior to identifying how you should handle an objection and implement tools offering data subjects the opportunity to submit an objection.

The processing activities that are justified by legitimate interests

Your company and data controllers processing data on behalf of your company are legally permitted to do so based on the following legitimate interests:

Processing of customer or client data (including direct marketing)

If there is an appropriate and relevant relationship between your company and/or data controllers acting on behalf of your company with the data subject, you may be able to apply the processing of customer or client data as a legitimate interest for processing that data. Use of the legitimate interest basis must be carefully assessed, and must include whether the data subject can reasonably expect at the point of data collection/submission that the data provided will be processed.

As previously outlined, utilising this category as a legitimate interest for processing data can be overridden in the event that the processing activity in question conflicts in any way with the personal rights or liberties of the data subject.

Your company must carefully consider whether to assume the processing of data applies to direct marketing activities. This can generally be applied through documentation; however, it is considered best practice under GDPR to obtain explicit consent for any processing activities associated with marketing (both direct and indirect).

Processing of data to ensure network or information security

There may be scenarios in which the processing of an individual's personal data is essential to ensure network security or information security. These activities must generally be carried out to prevent any potential data breaches or data security incidents that have the potential to

compromise the availability, the integrity or the confidentiality of data that is being stored or processed.

One-off data transfers

One-off data transfers are 'ad hoc' transfers that are not repetitive in nature. They tend to include only a limited number of data subjects. Use of one-off or ad hoc data transfer as a legitimate basis to support lawful processing. Again, this use of legitimate interest can be overridden in the event that such a data transfer conflicts with any one of the data subjects' personal liberties or rights under GDPR, the Data Protection Act 2018 or any other piece of legislation.

One-off data transfers must only be applied and carried out where no other grounds for transfer can be applied to the situation.

Assessing and communicating legitimate interests

It isn't enough to simply state your company's legitimate interest to support the lawful processing of data. Under GDPR legislation you must also undertake an assessment to clearly determine the legitimate interest as a legal basis for processing, as well as how and why it applies to the relevant activity.

This assessment, known as a legitimate interest assessment (LIA), should include be carried out in the following 3 steps:

1. You must identify the legitimate interest your company is choosing to apply
2. You must carry out a necessity test to decide whether the processing activity in question is necessary
3. You must carry out a balancing test to ensure the personal liberties and rights of the data subject do not outweigh the reasons your company has outlined as being necessary

Whilst there is no specific or formal format in which this assessment must be carried out, it is essential that each assessment includes the following information:

- Information regarding whether the data subject in question should reasonably expect the processing of their data, and why that expectation is present
- Information regarding whether the legitimate interests of your company and/or the data controller acting on behalf of your company are overridden by the individual rights or personal liberties of the data subject in question

When conducted correctly, a legitimate interests assessment will be able to prove that the privacy rights of any given data subject have been given due consideration prior to the carrying out of any processing activities.

If assessment of the scenario demonstrates that the data subject may not have had a reasonable expectation that their personal data would be processed for the activity in which you are attempting to apply it to, the individual's personal rights will outweigh your legitimate interests and the activity cannot and should not be carried out.

It's also worth noting that GDPR legislation includes transparency requirements dictating how you articulate and inform data subjects about the activities in which their personal data may be processed under relevant legitimate interests. Because individuals have a right to know how their personal data is being processed, your company has a legal obligation to communicate this in a clear and concise manner, which is easily accessible and easy to understand.

The information about legitimate interests your company applies can and should be included within your company's online privacy policy. For guidance on what to include in your privacy policy, please consult the Privacy statement and consent template.

12.EMPLOYEE CONSENT AND PRIVACY POLICY

Aims

Your company will need to collect certain personal information about the individuals working for it to carry out certain processes. This data could include information like health history, bank account details, marital status, home address and much more. As an employer, your company should go to great lengths to ensure that data is secure – and as a data controller adhering to GDPR rules, you have a range of legal obligations which apply to employee data.

To ensure your employees are informed about what data you're using, why you're using it and how it will be stored and processed, you should complete the enclosed employee privacy policy. Likewise, you should complete the enclosed employee consent template to collect the explicit consent of your employees, volunteers, contractors or anyone else associated with your company, stating that they agree for your company to collect, process and store their data.

Employee privacy policy

Here at Airport Transport Centre we take your privacy seriously. We greatly value your contribution to our success, and we will do everything we can to protect your individual rights and personal liberties.

As part of our ongoing relationship, we will need to collect, store and process certain information about you. This information is required to carry out certain processes, and we will clearly explain what those processes are and how your data will be used. You have the right to object to the processing of your data at any time.

This privacy policy may be occasionally updated in-line with company policy and regulatory updates. Any updates to this policy will be communicated to all employees as soon as possible.

How will your information be used?

As an employee of Airport Transport Centre we must store and process information about you for management and administrative use only. The information you give us will be stored and processed only to allow us to maintain an effective relationship with you as an employee. These management processes apply during the recruitment process, whilst you are an employee for Airport Transport Centre and when your relationship with our company has ended.

The management and administrative processes carried out using your data will allow us to adhere to the employee contract you have signed with us, as well as to comply with legal requirements we are duty-bound to follow. Your data may also be used to pursue the legitimate interests of Airport Transport Centre and to maintain any established position in the event of legal proceedings.

Most of the information our company holds relating to you has been provided to Airport Transport Centre by you. In some cases, we may also collect information about you from other internal sources such as a line manager. On other occasions we may collect and store information about you from external sources, such as a reference as part of the recruitment process.

If you don't want to provide us with the information requested, Airport Transport Centre might not be able to meet all of the obligations to you that we outlined in your employee contract. We will inform you in the event we are unable to comply with the conditions of your contract due to missing or withheld data.

We may anonymise your personal data in some cases so that it cannot be used to identify you. This may be done without notifying you.

After your relationship with our company has ended and you are no longer an employee at Airport Transport Centre we will store and/or securely destroy the data we hold relating to you in-line with applicable regulations.

There may be limited circumstances in which your data must be transferred outside of the EU. This will only ever be done to comply with our legal obligations, or our company's contractual obligations to you as our employee. To protect your personal data, Airport Transport Centre has implemented the following safeguards for data transfers:

- Consumer trends
- Consumer behavior
- Targeted discounts and future marketing.

Your personal data will be stored for a period of 6 months, unless otherwise noted. Criteria used for determining data retention for other situations are as follows:

- Consumer trends
- Consumer behavior
- Targeted discounts and future marketing.

There may also be situations in which your data is used as part of automated decision-making processes. Examples of these processes include profiling activity, as well as:

- Consumer trends
- Consumer behavior
- Targeted discounts and future marketing.

Our legitimate interests

Airport Transport Centre may occasionally need to process your data to pursue legitimate interests relating to our company and its business interests. Examples of situations in which we may process your personal data in the legitimate interests of the company include (but are not limited to):

- Fraud prevention
- Administrative purposes
- Crime reporting and detection

Our legitimate interests are to provide an unparallel service in transport market, and Airport Transport Centre will never use your information or wilfully process your data in any situation in which your own interests outweigh the legitimate interests of our company. We process your personal data only within our rights as enshrined in law, and we do so in a way that is transparent and fair.

We may occasionally need to process your data to ensure it is accurate and up-to-date or to ensure it is safe and secure.

What information do we collect?

Airport Transport Centre collects, stores and processes the following types of information about you as an employee:

- Your name
- Your title
- Your date of birth
- Your gender
- Your address
- Your telephone number(s)

- Your personal email address(es)
- Your marital status
- Information about dependents
- Your emergency contact information
- Your next of kin
- Your bank account details
- Your tax status information
- Your payroll records
- Your salary
- Information about your annual leave
- Your benefits information
- Your National Insurance number
- Your photograph
- Location of your employment or place of work
- A copy of your driving license
- A copy of your passport
- Your right to work documentation (if applicable)
- Your referees
- Your CV
- Your performance history
- Your disciplinary history
- Your grievance history
- CCTV footage (if applicable)
- Electronic key card records (if applicable)
- Information about your use of information systems

Why do we process your information?

Airport Transport Centre may process your data for the following reasons:

- To make a decision about your appointment
- To carry out payroll processes
- To provide you with benefits
- To liaise with your pension provider
- To administer other elements of your contract
- To manage performance
- To carry out accounting and auditing functions
- To assess your qualifications for a particular project, task or promotion
- To make a decision about salary reviews
- To make a decision about your continued employment

- To gather evidence about grievance or disciplinary hearings
- To address legal disputes
- To make a decision about terminating our relationship
- To assess your education or training requirements
- To manage your absences
- To ascertain your fitness to work
- To comply with health and safety obligations
- To carry out equal opportunities monitoring
- To prevent fraud
- To ensure network and information security
- To conduct data analytics

It is inevitable that in your capacity as an employee you will be referred to in company records. Please also note that wherever necessary, Airport Transport Centre may need to keep information relating to your health, such as reasons for absence and evidence of GP notes. This information will only ever be used to comply with our health and safety obligations and to administer benefits such as statutory sick pay.

If we need to process special categories of data, we will always obtain your explicit consent and explain for what purpose this information must be processed, unless this information is required to protect your health in an emergency, or if consent is not required by law.

Special categories of information may include (but are not limited to):

- Sexual orientation
- Racial or ethnic origin
- Political affiliations
- Religious affiliations
- Biometric data

Where consent is given to process this information, you reserve the right to withdraw your consent at any time.

We will only ever disclose information about you to external parties if Airport Transport Centre is legally obligated to do so, or in situations in which we must disclose your information to comply with our company's contractual obligations to you. Examples may include passing your contact details onto your pension provider. We may also transfer information about you to other companies within our wider family of companies, for purposes related to your employment or purposes related to company management and administration.

We may occasionally rely on profiling and/or automatic decision-making. This will only be used in certain limited situations:

- Consumer trends

- Consumer behavior
- Targeted discounts and future marketing.

We also monitor computer and telephone usage, to ensure that employment activities are carried out in-line with our Data Protection Policy and the Company Handbook.

To perform our contract with you or adhere to our legal requirements, your information may be transferred outside the EU or to global organisations. To ensure your data is protected, we have a list of security measures encrypted as per need information required to extend service Booked. A copy of these security measures can be requested from Airport Transport Centre.

We will store your personal information for a period of 6 months. We will also rely on the criteria outlined in the retention schedule when deciding how long to store your information. If we decide to store your personal information for a new reason, or a reason which differs from the one it was originally collected and stored for, the Data Protection Officer will provide you with this reason and any other accompanying information.

What are your rights?

Airport Transport Centre observes a host of regulatory obligations under the EU's GDPR legislation and the Data Protection Act 2018. As part of our ongoing commitment to preserve and uphold these regulatory commitments, we will also uphold your personal rights under these regulations.

Your statutory rights under GDPR and the Data Protection Act 2018 include:

- The right to request access to your personal information (also known as a 'data subject access request')
- The right to request corrections be made to the data we hold about you
- The right to request erasure of your personal data
- The right to object to the processing of your data
- The right to request any restrictions to the processing of your data
- The right to request the transfer of your data to another party

If you would like to exercise any of these rights, please contact Khawar Siddiqui in writing at Shelton Street, Covent Garden, WC2H 9JQ **OR** ksiddiqui@airporttransportcentre.com

You do not need to pay a fee to access the personal data we hold on you to exercise your rights under relevant data protection regulation; however, Airport Transport Centre reserves the legal right to charge a nominal fee for requests that are deemed to be unfounded or excessive in nature. We may also refuse to comply with requests that are deemed unfounded or excessive in-line with our own legal rights.

Please note that Airport Transport Centre may be required to collect more information about you to confirm your identity, before granting access to any information requested.

You have the right to issue a formal complaint to the Information Commissioner's Office at any time, if you feel Airport Transport Centre has not adequately complied with its requirements under GDPR or the Data Protection Act as they relate to the collection, storage, processing of your personal data, or your individual rights to access your data.

Who is Airport Transport Centre's Data Protection Officer?

Airport Transport Centre is the controller and processor of data. We collect, store and process data in accordance with our legal obligations under GDPR and the Data Protection Act 2018.

If you have any questions or concerns relating your information and the way we use it, please get in touch:

Khawar Siddiqui

ksiddiqui@airporttransportcentre.com

Airport Transport Centre

https://www.airporttransportcentre.com/

Signature _____ Date _____

Employer GDPR checklist

Complete this checklist to confirm you have reviewed your contracts and other documentation to include the relevant privacy notice and consent forms.