



Data Protection, including Privacy, Policy

BS ISO/IEC 27001:2013 and current version of PCI DS

DATA CLASSIFICATION

Public	✓
Internal	
Confidential	
Strictly Private	

Important: if you are in any doubt regarding how you should responsibly handle this document please refer to a senior member of staff

This Document is the property of Air Business Ltd and may not be copied, reproduced or released to any third party, without the permission of the Chief Executive Officer.

© Air Business, 2023

Data Protection, including Privacy, Policy - for Air Business Ltd

Dated 29 Mar 2023

Subscription Problem?

If you are here because of an issue with a subscription, please contact the publisher you have a contract with. We operate as a 'Processor' for the publisher, they are the 'Controller' responsible for your contract and your data.

Contents

Subscription Problem?	2
1. Who are we?	2
2. Who is this for?	2
3. Principles	3
4. More than just Privacy	3
5. Your Rights	4
6. Responsibilities	4
7. International Transfers	4
8. Definitions	5
9. Laws and Regulation	5

1. Who are we?

We are [Air Business Ltd](#), a market-leader in global mail, e-commerce, fulfilment, distribution and subscription management, and a wholly owned subsidiary of [An Post](#), the Irish Post Office.

Any questions or concerns relating to data protection with Air Business, or this policy, should be sent to: DPO@airbusiness.com. Or write to: The Data Protection Officer, Air Business Ltd, The Beacon, Mosquito Way, Hatfield, AL10 9WN.

If you are not satisfied with our response and you are resident in the EU you may also contact our EU Representative at privacyoffice@anpost.ie. Or write to: Data Privacy Office, An Post, Room 2-172, GPO, O'Connell Street Lower, Dublin 1, D01 F5P2.

If you continue to be dissatisfied, you have the right to complain to the UK data protection regulator, the Information Commissioner's Office (ICO): [Make a complaint | ICO](#).

2. Who is this for?

YOU. Everyone we process data for - or is responsible for processing personal data. We have one policy for all.

To deliver our services, we have to process personal data. To be successful, we have to do it right.

Protecting personal data has always been, and will always be, vital – for everyone, our staff, our customers and visitors. The General Data Protection Regulation (GDPR) describes how to do it legally right. We comply with the GDPR and related laws and regulations.

This Policy describes our intentions, *who* we are, *where* we operate, *how* we will protect your personal data, in line with GDPR, your legal rights, and how you can complain.

Data Protection Notices will notify you *what* data and processing we do, and *why*, as close as is reasonable to *when* you provide the data.

This Policy applies to all personal data processed by us (electronically & physically), and any person who processes or is the data subject of that data.

3. Principles

We wholeheartedly support the protection of “fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data” [Art.1\(2\)](#). That is why we seek full compliance with GDPR, related laws and regulations and train our staff to understand and actively maintain data protection. We know if we get it wrong it could hurt you, our people and our business – we are serious about data protection.

We are accountable for ensuring all ‘personal data’ is ‘processed’ ‘lawfully, fairly, in a transparent manner’ for a ‘specific purpose’ and not used for a purpose other than that for which it was collected (with very few lawfully permitted exceptions). We will ‘minimise data’ collection to only that necessary to achieve the stated purpose. We will ensure data ‘accuracy’, ‘integrity and confidentiality’, and ensure data is ‘available’ when needed, but only held for as long as necessary – then deleted (‘storage limitation’). In order to achieve this data will be encrypted during transmission and storage, and access time limited to authorised personnel only. This is a summary of GDPR Principles [Art.5](#).

Considering the Lawfulness of Processing ([Art.6](#)), most personal data we process is supplied under contract with another company, hence in most cases the ‘Lawful Basis’ is Contract. That’s also true for most personal data of our staff (employees, agency, contractors, consultants, etc.). On occasion a different, possibly additional, purpose may be applicable: Consent, Legal Obligation, Vital Interest, Public Interest or Legitimate Interest. We will inform you through the relevant Data Protection Notice.

To understand more, please read: [The principles | ICO](#), the [Lawful basis for processing | ICO](#), and [What is personal data? | ICO](#).

4. More than just Privacy

Privacy restricts who can see your data, that’s maintaining Confidentiality – but not what it is used for, how long it is kept, how it is stored, transmitted, or whether the use of your data is legal.

Data Protection gives you Privacy AND adds those protections.

The English word ‘Privacy’ is sometimes used when the legally accurate term is Data Protection. If we slip up and use the word ‘Privacy’, it should be taken to mean Data Protection, unless the context makes clear otherwise.

5. Your Rights

You have rights, as a living identified or identifiable natural person, to the 'personal data' that relates to you, the 'data subject'.

GDPR gives you these rights: to be informed about your data, access to your data, rectification of your data, erasure of your data, restricting the processing of your data, data portability, object to processing of your data and rights regarding automated decision making.

We fully support these rights. For more information see [Individual rights | ICO](#).

6. Responsibilities

If you work with, or for us, then it is your responsibility to actively comply with this policy and Data Protection laws and regulations.

If you are a customer or visitor, and you see a problem, please tell us immediately so we can fix it.

To support the principles above, we will:

- Fully comply with all aspects of GDPR and the law, not just this list or this policy.
- Provide you with clear information about who will use your personal data and how.
- Take special care when collecting data when it is 'special category' or from children.
- Maintain a Record of Processing Activities (RoPA) and categories of data stored.
- Delete data when no longer required; this might be later than you expect, as some types of data, especially financial and Human Resources (HR), must be held for several years.
- Ensure data processing is covered by a written contract.
- Provide additional contractual protections if we have to send data outside of the EEA or 'adequate countries' which have legal protections as strong as the EEA and UK.
- Provide relevant training to anyone who works with personal data to ensure adequate awareness, competence and capability.

7. International Transfers

Countries around the world have different laws and regulations regarding processing personal data. In most cases there is not the same concept of the 'rights and freedoms' and therefore not the same level of legal protection. It is important we get it right.

Although the UK GDPR applies only to the United Kingdom, it requires us to protect your data at all times and all places. We can't send it to somebody in another country unless we make sure your data will be safe.

The UK ICO has considered the data protection laws of countries around the world. Several countries have 'adequacy rulings' meaning personal data can be safely sent to them; this includes all EU and EFTA countries. The current UK adequacy list can be seen here: [International transfers | ICO](#).

The list does not currently include several important countries such as USA, India, Australia, Philippines, China (including Hong Kong), and only partially covers Canada and Japan. Any country without an 'adequacy ruling' is termed a 'Third Country'. As a matter of policy we will avoid sending personal data for processing to third countries, but it is not always possible.

When it is necessary to use a partner in a third country, we will take additional steps to protect personal data. We will carry out a Transfer Risk Assessment and if we are satisfied data can be

adequately protected with additional contractual protections, we will use the ICO approved International Data Transfer Agreement, or other ICO approved measures, which provides strong contractual protection.

8. Definitions

You will have noticed some words and phrases (terms) have ‘quote marks’ around them. This is to indicate they are legally important and are defined in GDPR.

Probably, the two most important terms are ‘Personal Data’ and ‘Processing’:

- ‘Personal Data’ means any information relating to an identified or identifiable natural person (‘data subject’). Note that personal data does not have to be capable of identifying the person, only that it is ‘relating to’ an identifiable person. This is a different to the American concept of Personally Identifying Information (PII).
- ‘Processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. This includes transmission, any sort of access (including viewing), storage and deletion.

These are shortened definitions, please read GDPR [Article 4 - Definitions](#) for the full definition of these and other terms.

9. Laws and Regulation

As a UK registered company, and the UK no longer being in the EU, only UK Law applies. The UK General Data Protection Regulation (UK GDPR) describes data protection; it is almost the same as the EU GDPR. You can read the [UK GDPR Updated for Brexit | UK GDPR \(uk-gdpr.org\)](#).

These sections are key to understanding GDPR, and rather than repeating it here and making a long document even longer, please follow the links:

- [Article 4](#) provides definitions, see especially ‘Personal data’ and ‘Processing’
- [Article 5](#) states limitations on how data may be processed
- [Article 6](#) specifies the six lawful conditions for processing
- [Chapter 3](#) (articles 12-23) describe your rights

In addition to UK GDPR, websites and other electronic communications are also subject to PECR: [The Privacy and Electronic Communications \(EC Directive\) Regulations 2003](#) - this will often impact sales and marketing.

Any update, change or replacement of the regulation and law will also automatically apply in the timescales specified by the UK Government.

The original EU GDPR can be found here: [General Data Protection Regulation \(GDPR\) – Official Legal Text \(gdpr-info.eu\)](#). In common with other EU legislation, and unlike UK law, the reasons for the creation of the regulation are specified in some detail in the section called ‘[Recitals](#)’; this can aid understanding.

Authoritative source

We have tried to make this policy as easy to read as possible and linked to similarly easy to read texts. The actual law is the [Data Protection Act 2018 \(legislation.gov.uk\)](#) which enacts the UK GDPR: [Regulation \(EU\) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the](#)

[protection of natural persons with regard to the processing of personal data and on the free movement of such data \(United Kingdom General Data Protection Regulation\) \(Text with EEA relevance\) \(legislation.gov.uk\)](#). The following 'Brexit' legislation made the changes from EU to UK: [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2019 \(legislation.gov.uk\)](#)