

GDPR Compliance Statement

(ISO 27001:2022 Organisational Controls – Clause 5.34)

Author	Greg Nott
Version	2.0
Date Created	23/05/2024
Last Update Date	30/10/2024
Document Control	Released
Document ID	240523-IMS-POL-GDPRComplianceStatement-V2
Security Classification	Public

Table of Contents

GDPR Compliance Statement	1
Approval.....	3
Review.....	3
Change History.....	3
Associated Documents.....	3
Scope.....	4
Introduction	4
Our GDPR Commitment.....	4
Data Audit	4
Privacy Policy	4
International Data Transfers.....	4
Data Processing Agreements	5
Data Security.....	5
Data Protection Impact Assessments	5
Data Breach Protocol	5
Data Retention	5
Legal Bases and Consent.....	5
Data Subject Rights	6
Data Protection Officer	6

Approval

Author	Issue	Approved By	Date
Greg Nott	1.0	Sharon Benning-Prince	23-May-24
Greg Nott	2.0	Sharon Benning-Prince	30-Oct-24

Review

Reviewer	Review Criteria	Issue	Date
Sharon Benning-Prince	ISO 27001:2022	1.0	23-May-24
Sharon Benning-Prince	ISO 27001:2022	2.0	30-Oct-24

Change History

Author	Change	Issue	Date
Greg Nott	Creation	1.0	19-May-24
Greg Nott	Address Change	2.0	30-Oct-24

Associated Documents

Document	Version
230527-IMS-POL-PrivacyByDesign-V2	2.0
230520-IMS-POL-TransparencyAndPrivacyPolicy-V4	4.0

Scope

This document is part of the Integrated Management System (IMS) for ARO and is consistent with the standards listed below and describes the Transparency & Privacy Policy adopted by ARO.

- ISO 27001:2022 – Information Security Management Systems
 - ISO 27017:2015 – Code of Practice for Cloud Services
 - ISO 27018:2020 – Code of Practice of Personally Identifiable Information (PII)
- ISO 9001:2015 – Quality Management System
- DSPT (Data Security and Protection Toolkit) for the NHS.
- Cyber Essentials Plus

This policy applies to all activities undertaken by ARO in the processing of Personally Identifiable Information (PII) during the course of its operations.

This policy should be read in conjunction with our Transparency and Privacy policy.

Introduction

As a leading IT Managed Service Provider (MSP) based in the UK, ARO is dedicated to protecting the privacy and security of our employees and customers data. We have been fully compliant with the General Data Protection Regulation (GDPR) since its enforcement on 25 May, 2018. Our adherence to GDPR standards reflects our commitment to safeguarding personal data and maintaining the highest standards of data privacy and security.

Our GDPR Commitment

ARO is committed to upholding the principles of GDPR, ensuring that all personal data is processed lawfully, fairly, and transparently. We prioritise the privacy and security of our customers' data, implementing rigorous measures to protect it.

Data Audit

We have conducted a comprehensive audit of all personal data held by ARO. This audit involved identifying all data sources, mapping data flows, and documenting data processing activities to ensure compliance with GDPR.

Privacy Policy

We have updated our Privacy Policy to reflect our GDPR compliance. Our policy provides clear and transparent information about how we collect, use, store, and protect personal data, ensuring that individuals are fully informed about their data rights.

International Data Transfers

When transferring personal data out of the EU, we implement appropriate safeguards, such as Standard Contractual Clauses (SCCs), to ensure the protection of personal data. We also apply additional measures where necessary to comply with GDPR requirements.

Data Processing Agreements

We have established Data Processing Agreements (DPAs) with all partners and third-party service providers. These agreements ensure that our partners adhere to GDPR standards and protect personal data in line with our rigorous requirements.

Data Security

ARO employs robust technical and organisational measures to ensure data security, including encryption, pseudonymization, and regular security assessments. We are independently certified to the following standards:

- ISO 27001:2022 – Information Security Management Systems, including:
- ISO 27017:2015 – Code of Practice for Information Security Controls for Cloud Services
- ISO 27018:2020 – Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds
- NHS Data Security & Protection Toolkit (DSPT)

These standards demonstrate our commitment to maintaining the highest level of information security management.

Data Protection Impact Assessments

We conduct Data Protection Impact Assessments (DPIAs) for new data processing activities or technologies to assess and mitigate potential privacy risks. This proactive approach ensures that we remain compliant with GDPR and protect personal data effectively.

Data Breach Protocol

We have established a comprehensive procedure for identifying, assessing, and reporting data breaches. In the event of a breach, we will promptly notify affected individuals and relevant authorities as required by GDPR.

Data Retention

Our data retention practices have been reviewed and updated to ensure that personal data is retained only as long as necessary for the purposes for which it was collected and in accordance with legal requirements.

Legal Bases and Consent

Most of our data processing activities at ARO are based on legitimate business interests, ensuring that we provide the best possible services to our clients while maintaining compliance with GDPR. We carefully assess and balance our legitimate interests against the rights and freedoms of data subjects, ensuring that their privacy is not compromised.

In instances where processing is not based on legitimate interests, we ensure that we obtain GDPR-compliant consent from individuals before collecting or processing their personal data. Our consent mechanisms are clear, specific, and require affirmative action from the data subject. We also make it easy for individuals to withdraw their consent at any time.

Data Subject Rights

ARO facilitates data subject rights requests, ensuring that individuals can easily exercise their rights to access, rectify, erase, restrict, and object to the processing of their personal data. We also support data portability requests.

Data Protection Officer

We have appointed a Data Protection Officer (DPO) to oversee our data protection strategy and implementation. Our DPO can be contacted at:

- **Name:** Greg Nott
- **Role:** Head of Information Security
- **Email:** dpo@aro.tech
- **Phone:** 0330 440 4444
- **Address:** Arrow Business Communications Limited, trading under the brand name ARO
Kilby House
Liverpool Innovation Park
Liverpool
L7 9NJ

ARO is fully committed to GDPR compliance, ensuring the highest standards of data privacy and security. Through comprehensive audits, updated policies, robust security measures, and clear communication, we protect personal data and uphold the rights of data subjects. Our dedicated Data Protection Officer is available to address any questions or concerns regarding our data protection practices.