



## GDPR Policy

**Document Title: GDPR Policy**




**Document Number: ATMS-POL-PRO-070**

**Document Number: A01**

**Date: Tuesday, 13 April 2021**

### Document Control

Document/Report Title:	GDRP Policy
Document/Report No:	ATMS-POL-PRO-070
Document/Report Version:	A01

Issue/Amendment	Prepared	Checked	Approved
First Issue A01	Name and position: Emma Littlewood Office Manager Signature:  Date: 13/04/2021	Name and position: Nicholas Carter Managing Director Director Signature:  Date: 13/04/2021	Name and position: Nicholas Carter Managing Director Director Signature:  Date: 13/04/2021

## Contents

<b>1.0</b>	<b>Executive Summary</b> .....	<b>3</b>
<b>2.0</b>	<b>Purpose</b> .....	<b>3</b>
<b>3.0</b>	<b>Scope</b> .....	<b>3</b>
<b>4.0</b>	<b>Policy Statement</b> .....	<b>3</b>
<b>5.0</b>	<b>Commitment</b> .....	<b>3</b>
<b>6.0</b>	<b>Implementation</b> .....	<b>3</b>
<b>7.0</b>	<b>Principles</b> .....	<b>4</b>
<b>8.0</b>	<b>Principles Rights of Individuals</b> .....	<b>4</b>
<b>9.0</b>	<b>Roles and Responsibilities</b> .....	<b>4</b>
<b>10.0</b>	<b>Approach</b> .....	<b>6</b>
<b>11.0</b>	<b>Policy Breach</b> .....	<b>6</b>
<b>12.0</b>	<b>Transfer of Personal Information to Third Parties</b> .....	<b>6</b>
<b>13.0</b>	<b>Policy Review and Revision</b> .....	<b>7</b>
<b>14.0</b>	<b>Complaints</b> .....	<b>7</b>

## 1.0 Executive Summary

This policy documents ATMS EMCS Ltd. GDPR Policy.

## 2.0 Purpose

In order for ATMS EMCS Ltd. to operate and achieve its business objectives it needs to collect, process and store personal information relating to its employees (prospective, present and past), tenants, authorised users, members of the public, suppliers, contractors and other key stakeholders.

ATMS EMCS Ltd. is committed to complying with data protection legislation, as well as other relevant privacy legislation.

The purpose of this policy is to:

- Outline the way ATMS EMCS Ltd. will process personal information to achieve compliance with relevant data protection and privacy legislation.
- Inform ATMS EMCS Ltd. personnel of their responsibilities when processing personal information.

## 3.0 Scope

This policy applies to everyone that works for or on behalf of ATMS EMCS Ltd, in every joint venture company under ATMS EMCS Ltd. control, and to those working in a ATMS EMCS Ltd. under any alliance. This includes, but is not limited to, employees (full and part time), contractors, secondees, agency staff, suppliers, consultants and agents.

## 4.0 Policy Statement

We aim to enhance the reputation of ATMS EMCS Ltd. by handling all company personnel personal information fairly and securely and in compliance with the law. ATMS EMCS Ltd. is required to comply with various pieces of data protection legislation, this includes but is not limited to:

- The General Data Protection Regulation.
- The Data Protection Act 2018.
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended).
- The Human Rights Act 1998.
- The Networks and Information Systems Directive (NIS Directive) 2018.

## 5.0 Commitment

ATMS EMCS Ltd. recognises and respects every individual's rights to the protection of personal data. We are committed to meeting our legal and regulatory obligations and will adhere to the EU General Data Protection Regulation (GDPR) and the specific provisions of the UK Data Protection Bill.

## 6.0 Implementation

Our Directors are responsible for the effective implementation and maintenance of data protection management through all areas of the business. All staff will comply with the data protection directives

and follow the guidance provided and will not unlawfully process or share the personal data of individuals.

## 7.0 Principles

Data protection legislation contains certain principles regarding the handling of personal information. ATMS EMCS Ltd. must comply with the following principles relating to processing of personal information. Personal information must be:

- Processed fairly, lawfully and transparently.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Adequate, relevant and limited to what is necessary for the purposes for which it is processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal information that is inaccurate is either erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information is processed.
- Processed in a manner that ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

## 8.0 Principles Rights of Individuals

Data Protection law also provides the following rights for individuals:

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.

Rights in relation to automated decision making and profiling ATMS EMCS Ltd. has implemented processes and procedures to enable compliance with the rights of individuals. If you receive a request from an individual, you should contact the Directors who will be able to advise you of your responsibilities in complying with these rights.

## 9.0 Roles and Responsibilities

The Directors are ultimately accountable for ensuring that ATMS EMCS Ltd. meets its legal obligations under data protection legislation, and it is the responsibility of its members to:

- Oversee completion of data protection risk assessment(s) throughout their directorate.

- Oversee the appointment of Data Protection leads in high risk areas and, where required, the provision of appropriate improvement action plans.

It is the responsibility of the Group General Counsel to:

- Monitor the enterprise risk within corporate appetite through the Business Director Committee
- Provide assurance to the Executive Committee and Board on business compliance.

It is the responsibility of the Directors to:

- Own and regularly review the data protection policy.
- Set the overall strategic approach for data protection compliance.
- Direct activity to support business compliance with the policy.

It is the responsibility of the Directors to implement the Data Protection Strategy and Data Protection Compliance Plan, including:

- Review the implementation and effectiveness of the Data Protection policy on a regular basis.
- Provide advice and guidance to the business to ensure compliance with this policy.
- Be the central point of contact for the Information Commissioner's Office and, when appropriate, report Personal Information incidents to them.

Each high-risk business area (as defined on the completion of a data protection risk assessment) must appoint a Data Protection lead.

It is the responsibility of the Data Protection Leads to:

- Provide assurance to the Directors, that the Ethics and Data Protection is compliant with the policy.
- Refresh the high-level Data Protection risk assessment on an annual basis.
- Put in place an appropriate improvement action plan and oversee delivery of improvement actions.
- Be an advocate for data protection in their business area, including encouraging take up of e-learning.
- Escalate issues to the central Directors where required.

It is the responsibility of Line Managers to:

- Disseminate and implement this policy throughout their reporting lines.
- Investigate any incident involving personal information with assistance from the HR Director and other suitably skilled personnel.

It is the responsibility of everyone working for, or on behalf of Company to:

- Complete the provided 'E-learning' or briefing Data Protection training.

- Manage and handle personal information in accordance with the data protection principles contained within this policy as well as any associated standards, policies, guidance and procedures.
- Classify and label personal information appropriately.
- Undertake Data Protection Impact Assessments as appropriate, and in accordance with the Data Protection Impact Assessment guidance review on a regular basis the adequacy of security measures implemented to protect personal information in conjunction with Information Security (e.g. permission or access, particularly noting any personnel changes).
- Report any personal information incident or suspected personal information incident to the Directors or Line Manager immediately.
- Securely dispose of personal information once it has reached the end of its useful life and in line with the requirements of the Confidentiality Policy.

## 10.0 Approach

We ensure that all processing of personal data performed by us, or our third-party providers, has a lawful basis, and will always balance our interests against the interests, rights, and freedoms of the individuals. We operate a risk-based approach to the protection of personal data, ensuring that processing is designed with appropriate technical and organisational measures, such that we are effectively safeguarding personal data and the rights of data subjects.

We ensure that processes are in place to deal with the individual data subject rights under the GDPR, and that all staff are aware of these processes and are able to respond to data subject requests efficiently and effectively. We are able to evidence compliance, demonstrating that our use of personal data is lawful, is limited to the purpose for which it was originally collected, is relevant and necessary, is complete and up-to-date, is retained for only as long as is necessary, and is adequately secure.

## 11.0 Policy Breach

In the event you become aware this policy has been, or may have been breached, please contact the HR Director immediately.

Failure to comply with this policy may constitute a breach of terms and conditions of employment or contract and can lead to legal or disciplinary action up to and including dismissal or termination of contract.

If a criminal offence has been committed, further action may be taken to assist in the prosecution of the offender(s).

## 12.0 Transfer of Personal Information to Third Parties

Where transfers of personal information are to a third parties takes place, this must only take place where certain conditions are complied with. In this instance employees should seek confirmation of the adequate safeguards the supplier can provide.

This might include, but is not limited to:

- A legally binding agreement between companies or bodies.
- Binding corporate rules – agreements governing transfers made between organisations within a corporate group.

### 13.0 Policy Review and Revision

This policy has been approved by the ATMS EMCS Ltd. Directors and will be reviewed on an annual basis.

### 14.0 Complaints

If you are dissatisfied with the way your personal information is handled within ATMS EMCS Ltd. in the first instance you should discuss this with your Line Manager or the Directors.

Any investigations which take place as a result of a complaint will be handled by the relevant Line Manager or Director in consultation with the ATMS EMCS Ltd. legal team.