ADVANCED
ACCESS PLATFORMS

Advanced Access Platforms - GDPR Policy

Advanced Access Platforms (AAP) needs to collect person-identifiable information about individuals in order to carry out its functions and fulfil its objectives. Personal data is defined as 'information which relates to a living individual and from which they can be identified, either directly or indirectly'.

Personal data at AAP can include employees, customer, suppliers and third parties, private and confidential information as well as sensitive information, whether on paper, in electronic or other form.

Irrespective of how the information is collected, recorded and processed, person identifiable information must be dealt with properly to ensure compliance with the GDPR and the DPA.

They require AAP to comply with the seven principles relating to the processing of personal data (Appendix A). Under the Data Protection (Charges and Information) Regulations 2018, organisations that determine the purpose for which personal data is processed must pay the Information Commissioner's Office (ICO) a fee unless they are exempt. This new fee replaces the requirement to 'notify' or 'register', required under the old data protection regime.

Data protection legislation gives rights to data subjects (people that we hold information about) to access their own personal information, to have it corrected if wrong, in certain permitted circumstances ask us to erase it or stop using it and to seek damages where we are using it improperly.

The lawful and correct treatment of person-identifiable information by AAP is paramount to the success of the organisation and to maintaining the confidence of its employees, stakeholders and service users. This policy will help AAP ensure that all person-identifiable information is handled and processed lawfully and correctly.

GDPR/DPA principles
AAP has a legal obligation to comply with all relevant legislation in respect of data protection and information and IT security. The organisation will refer relevant guidance issued by advisory groups and professional bodies.

All legislation relevant to an individual's right to the confidentiality of their information and the ways in which that can be achieved and maintained are paramount to AAP. Significant penalties can be imposed upon the organisation or its employees for non-compliance.

1 Kimpton Road, Sutton, Surrey SM3 9QL
Tel: 020 8641 7050
E: info@advancedaccessplatforms.co.uk
www.advancedaccessplatforms.co.uk

The purpose of this policy is to outline how AAP meets its legal obligations in safeguarding confidentiality and adheres to information security standards. The obligations within this policy are principally based upon the requirements of the GDPR, as the key legislative and regulatory provision governing the security of person-identifiable information.

Other relevant legislation and guidance referenced and to be read in conjunction with this policy, is outlined together with a brief summary at Appendix B.

What information is covered?

Personal data within the respective legislative and regulatory provisions covers 'any data that can be used to identify a living individual either directly or indirectly'. Individuals can be identified by various means including but not limited to, their address, telephone number or e-mail address. Anonymised or aggregated data is not regulated by the provisions, providing the anonymisation or aggregation of the data is irreversible.

Policy statement
This document defines the data protection policy for AAP. It applies to all person-identifiable information obtained and processed by the organisation and its staff.

It sets out:

the organisation's policy for the protection of all person-identifiable information that is processed
establishes the responsibilities (and best practice) for data protection
references the key principles of the GDPR.
Principles
The objective of this policy is to ensure the protection of AAP's information in accordance with relevant legislation, namely:

To ensure payment of processing fee

Pay annually, the relevant processing fee to the Information Commissioner's Office in respect of the person-identifiable information AAP processes.

To ensure professionalism

All information is obtained, held and processed in a professional manner in accordance with the six principles of the GDPR.

To preserve security

All information is obtained, held, disclosed and disposed of in a secure manner.

To ensure awareness

Provision of appropriate training and promote awareness to inform all employees of their responsibilities.

Data Subject's rights request

Prompt and informed responses to a subject's rights request.

The policy will be approved following annual review. Where review and update is necessary due to legislative changes this will be done immediately.

In accordance with the AAP's equality and diversity policy statement, this procedure will not discriminate, either directly or indirectly, on the grounds of gender, race, colour, ethnic or national origin, sexual orientation, marital status, religion or belief, age, union membership, disability, background or any other personal characteristic.

Scope of this policy

This policy will ensure that person-identifiable information is processed, handled, transferred, disclosed and disposed of lawfully. Person-identifiable information should be handled in the most secure manner by authorised staff only, on a need-to-know basis.

The procedure covers all person-identifiable information whether clinical or nonclinical, electronic or paper which may relate to individuals, employees, contractors or third parties about whom we hold information.

Policy
The AAP obtains and processes person-identifiable information for a variety of different purposes, including but not limited to:

staff and administrative records matters relating to the prevention, detection and investigation of fraud and corruption, complaints and requests for information. Such information may be kept in either computer or manual records. In processing such personal data AAP will comply with the data protection principles set out in the GDPR/DPA.

Data protection responsibilities
Overall responsibilities
The AAP Board, collectively known as the 'data controller' permit the organisation's staff to use computers and relevant filing systems (manual records) in connection with their duties. The Board have a legal responsibility for the payment of the processing fee and compliance with the GDPR.

The Board whilst retaining their legal responsibilities have delegated data protection compliance to the Data Protection Officer.

Data Protection Officer's (DPO) responsibilities
The Data Protection Officer's responsibilities include:

- ensuring that the policy is produced and kept up to date
- ensuring that the appropriate practice and procedures are adopted and followed by AAP.
- provide advice and support to the Board on data protection issues within the organisation
- work collaboratively with Organisational Development and Governance and Assurance to help set the standard of data protection training for staff
- ensure the processing of personal information is reviewed and advise the organisation on the appropriate processing fee to be paid to the ICO
- ensure compliance with individual rights requests
- act as a central point of contact on data protection issues within the organisation.
- implement an effective framework for the management of data protection.

Line managers' responsibilities

All line managers across the organisation's business units are directly responsible for ensuring their staff:

- are made aware of this policy and any notices.
- are aware of their data protection responsibilities.
- receive suitable data protection training.

General responsibilities

All AAP staff, including temporary and contractors are subject to compliance with this policy. Under GDPR, individuals as 'processors' working on the 'controller's' behalf can be held personally liable for data protection breaches, especially where they have received the requisite training.

All AAP staff have a responsibility to inform their business unit Leads and the DPO of any new use of personal data, as soon as reasonably practicable after it has been identified.

All AAP staff will, upon receiving a rights request from an individual for information or concerns about the processing of personal information, should immediately forward the request to the Information Governance Team at HR@advancedaccessplatforms.co.uk.

Staff must follow the organisation's rights request procedure (see Appendix C).

Monitoring

Compliance with this policy will be monitored by the Finance and Corporate Governance Unit and may be subject to periodic internal or external audit review where necessary.

The Information Governance and Risk Management Lead is responsible for the monitoring and updating of this policy document.

Validity of this policy

This policy will be reviewed at least on a biennial basis or sooner, should the need arise under the authority of the Board. Associated data protection standards will be subject to ongoing development and review.

John Corcoran
Managing Director

January 2023