ASDAN GDPR Policy

Key details

Policy owner: Paul Sinclair	Current policy date: April 2018
	Next review date: April 2020

Introduction

ASDAN needs to gather and use certain information about individuals in order to conduct its business. These can include students, customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This policy ensures ASDAN:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The General Data Protection Regulation describes how organisations – including ASDAN – must collect, handle and store personal information.

The legislation applies regardless of whether data is stored electronically, on paper or on other materials.

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

People, risks and responsibilities

Policy scope

This policy applies to:

- The head office of ASDAN
- All sub offices of ASDAN
- All staff of ASDAN
- All contractors, suppliers and other people working on behalf of ASDAN

It applies to all data that the company holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Date of birth

- Gender

Data protection risks

This policy helps to protect ASDAN from data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could breach GDPR if hackers successfully gained access to sensitive data.

As part of GDPR readiness, a full data audit has been conducted and a record of where and how all personal data is collected and shared is available on the GDPR wiki page.

In order to ensure we follow data protection by design and by default, all new IT projects must have a Privacy Impact Assessment conducted in order to determine if personal data is being collected or shared and therefore needs to be assessed and audited.

Responsibilities

Everyone who works for or with ASDAN has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **Directors** are ultimately responsible for ensuring that ASDAN meets its legal obligations.
- The **Data Protection Officer** is responsible for:
    - Keeping the board updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data ASDAN holds about them ('subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- The **IT manager** is responsible for:

  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

- The **Design and Communications team** is responsible for:

  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff responsibilities

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **ASDAN will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where personal data should be safely stored. Questions about storing data safely can be directed to the IT manager.

When data is **stored on paper,** it will be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data must be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media,** these will be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to **approved cloud computing services**.
- Servers containing personal data are **sited in a secure location**, away from general office space.
- Data is be **backed up daily**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by unencrypted email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT team can explain how to send data to authorised external contacts.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data accuracy

The law requires ASDAN to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort ASDAN should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is up to date.** For instance, by confirming a customer's details when they call.
- ASDAN will make it **easy for data subjects to update the information** ASDAN holds about them. For instance, via the ASDAN website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Information requests

All individuals who are the subject of personal data held by ASDAN are entitled to:

- Confirmation that their personal data is being processed and why
- Ask what information the company holds about them and why including
    - The categories of personal data involved
    - Who the information has been, or will be, disclosed to
    - The length of time the data will be held for
    - Who provided the information (if not the individual themselves)
    - Whether their data is involved in automated decision-making such as profiling
    - Ask how to gain access to personal data
- Be informed on how to keep personal data held up to date
- Be informed on how ASDAN is meeting its data protection obligations including access to ASDAN's Privacy Notice

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests should be made by email via info@asdan.org.uk, addressed to the DPO. The DPO will verify the identity of the individual before providing the information requested by email within 14 working days. All requests will be recorded on the Information Request Log including the outcome and explanatory notes if necessary. Emails received in relation to an

Information Request will be held for one year from the date the enquiry has been satisfied in order to track repeat or nuisance requests, which may incur an administrative charge.

Enquiries received from centres requesting copies of details held in relation to past or current candidates will not be considered Information Requests and will be dealt with in accordance with Centre Support procedures and ASDAN's Privacy Notice.

In all cases, it is essential that the identity of the person requesting the information must be verified by reasonable means before any personal data is shared.

Disclosing data for other reasons

In certain circumstances, the General Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, ASDAN will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Privacy Notice

ASDAN aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, ASDAN has a privacy statement, setting out how data relating to individuals is used by the organisation and which other organisations learner data is shared with.

Email guidance

ASDAN staff should refer to the company's Email Policy documentation.

Breach Procedure

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, or an incident that affects the confidentiality, integrity or availability of personal data whether accidental or deliberate. This includes incidents in which data is accessed or passed on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

ASDAN's Breach Procedure must be followed whenever a personal data breach of any kind is identified. ASDAN staff should refer to the company's Breach Procedure documentation.