DATA PROTECTION POLICY

Last updated: 5th March 2018

1. Context and overview

1.1 Key details:
Approved by management on: 5th March 2018.
Policy became operational on: 5th March 2018.
Next review date: 1st March 2019.

1.2 Introduction

Advanced Witness Systems Ltd needs to gather and use certain information about individuals. These can include 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 is collected, handled and stored to meet the company's data protection standards — and to comply with the General Data Protection Regulation, GDPR.

1.3 This data protection policy ensures Advanced Witness Systems Ltd:

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

2. People, risks and responsibilities

2.1 Policy scope

This policy applies to:

a) The head office of Advanced Witness Systems Ltd
b) All trading names of Advanced Witness Systems Ltd, including TESCA Consultancy and Advanced Data & Measurement Systems
c) All staff and volunteers of Advanced Witness Systems Ltd
d) All contractors, suppliers and other people working on behalf of Advanced Witness Systems Ltd

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the General Data Protection Regulation. This may include:

a) Names of individuals
b) Postal addresses
c) Email addresses
d) Telephone numbers
e) …plus any other information relating to individuals

2.2 This policy helps to protect Advanced Witness Systems Ltd from data security risks, including:

a) Breaches of confidentiality.
b) Failing to offer choice.
c) Reputational damage.

2.3 Responsibilities

Everyone who works for or with Advanced Witness Systems Ltd has some responsibility for ensuring data is collected, stored and handled appropriately. Personal data will be handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

a) The Managing Director is ultimately responsible for ensuring that Advanced Witness Systems Ltd meets its legal obligations.
b) The data protection officer, in this case the Managing Director, is responsible for:
    i. Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    ii. Arranging data protection training and advice for the people covered by this policy.
    iii. Handling data protection questions from staff and anyone else covered by this policy.
    iv. Dealing with requests from individuals to see the data Advanced Witness Systems Ltd holds about them (also called 'subject access requests').
    v. Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    vi. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    vii. Performing regular checks and scans to ensure security hardware and software is functioning properly.
    viii. Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
    ix. Approving any data protection statements attached to communications such as emails and letters.
    x. Addressing any data protection queries from journalists or media outlets like newspapers.
    xi. Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

3. General staff guidelines

a) The only people able to access data covered by this policy will be those who need it for their work.
b) Data will not be shared informally. When access to confidential information is required, employees can request it from their manager.
c) Advanced Witness Systems Ltd will provide training to all employees to help them understand their responsibilities when handling data.
d) Employees will keep all data secure, by taking sensible precautions and following the guidelines below.
e) In particular, strong passwords will be used and will never be shared with unauthorised employees or 3rd parties.
f) Personal data will not be disclosed to unauthorised people, either within the company or externally.
g) Data will be reviewed and updated if it is found to be out of date. If no longer required, it will be deleted and disposed of.
h) Employees should request help from their manager or the data protection officer if they are unsure about any aspect of data protection.

4. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data controller. 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:

a) When not required, the paper or files will be kept in locked storage.
b) Employees will make sure paper and printouts are not left where unauthorised people could see them.
c) Data printouts will be shredded and disposed of securely when no longer required.

When data is stored electronically, it will be encrypted to protect from unauthorised access, accidental deletion and malicious hacking attempts:

a) Data will be protected by strong passwords.
b) If data is stored on removable media (like a CD or DVD), these will be encrypted, and kept locked away securely when not being used.
c) Data will only be stored on designated encrypted drives and servers, and will only be uploaded to an approved cloud computing services.

d) Servers containing personal data are sited in a secure location, away from general office space.
e) Data will be backed up frequently. These backups will be encrypted in line with the company's standard backup procedures.
f) All servers and computers containing data are protected by approved security software and a firewall.

5. Data use

To ensure personal data is kept safe:

a) When working with personal data, screens of computers are always locked when left unattended.
b) Personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
c) Data must be encrypted before being transferred electronically.
d) Employees will not save copies of personal data to their own computers.

6. Data accuracy

The law requires Advanced Witness Systems Ltd to take reasonable steps to ensure data is kept accurate and up to date. 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.

a) Data will be held in as few places as necessary.
b) Staff should take every opportunity to ensure data is updated.
c) Advanced Witness Systems Ltd will make it easy for data subjects to update the information Advanced Witness Systems Ltd holds about them.
d) Data will be updated as inaccuracies are discovered.

7. Subject access requests

All individuals who are the subject of personal data held by Advanced Witness Systems Ltd are entitled to:

a) Ask what information the company holds about them and why.
b) Ask how to gain access to it.
c) Be informed how to keep it up to date.
d) Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data controller at gdpr@awstorque.co.uk. The data controller can supply a standard request form, although individuals do not have to use this. Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

8. Disclosing data for other reasons

In certain circumstances, the General Data Protection Regulation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Advanced Witness Systems Ltd will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the company's legal advisers where necessary.

9. Providing information

Advanced Witness Systems Ltd aims to ensure that individuals are aware that their data is being processed, and that they understand:
a) How the data is being used
b) How to exercise their rights

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company. This is available on request. A version of this statement is also available on the company's website.