Association of Women Solicitors London
Data protection policy

This is the Data Protection Policy of the Association of Women Solicitors London (AWSL) and gives important information about:

- the data protection principles with which the AWSL must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept; and
- your rights

1 Introduction

1.1 AWSL obtains, keeps and uses personal information (also referred to as data) about members, and other individuals who have agreed to receive information about AWSL. Personal data is held by AWSL for a number specific lawful purposes, as set out in the AWSL's data protection privacy notice.

1.2 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to you. Its purpose is also to ensure you understand how we collect, use and manage personal information that we receive.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information and how (and when) we delete that information once it is no longer required.

1.4 Linda Davies is responsible for data protection compliance within the AWSL. If you have any questions or comments about the content of this policy or if you need further information, you should contact Linda Davies on AWSLondon1@gmail.com.

2 Scope

2.1 This policy applies to your personal information

2.2 You should refer to the AWSL's Privacy Notice and, where appropriate, to its other relevant policies including in relation to information retention and security, which contain further. information regarding the protection of personal information in those contexts.

3 Definitions

AWSL	the Association of Women Solicitors' London;
Committee	the committee of AWSL appointed or co-opted in accordance with the AWSL constitution;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

4 Data protection principles

4.1 AWSL will comply with the following data protection principles when processing personal information:

4.1.1 we will process personal information lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

4.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;

4.1.5 we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and

4.1.6 we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5 Basis for processing personal information

5.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

5.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which the AWSL is subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person;

(e) that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or

(f) that the processing is necessary for the purposes of legitimate interests of the AWSL or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 5.2 below.

5.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

5.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
5.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
5.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 6 below), and document it; and
5.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

5.2 When determining whether the AWSL's legitimate interests are the most appropriate basis for lawful processing, we will:

5.2.1 conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
5.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
5.2.3 keep the LIA under review, and repeat it if circumstances change; and
5.2.4 include information about our legitimate interests in our relevant privacy notice(s).

6 Special category personal data

6.1 Special categories of personal data are sometimes referred to as 'sensitive personal data'.
6.2 AWSL will not process any special category personal data. If this changes, our members will be notified of the lawful basis under which we need to do this.
6.3 The AWSL will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.

7 Data protection impact assessments (DPIAs)

7.1 Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the AWSL is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

7.1.1 whether the processing is necessary and proportionate in relation to its purpose;
7.1.2 the risks to individuals; and
7.1.3 what measures can be put in place to address those risks and protect personal information.

8 Documentation and records

8.1 We will keep written records of processing activities, including:

8.1.1 the purposes of the processing;
8.1.2 a description of the categories of individuals and categories of personal data;
8.1.3 categories of recipients of personal data;
8.1.4 where possible, retention schedules; and
8.1.5 where possible, a description of technical and organisational security measures.

8.2 As part of our record of processing activities we document, or link to documentation, on:

8.2.1 information required for privacy notices;
8.2.2 records of consent;
8.2.3 controller-processor contracts;
8.2.4 the location of personal information;
8.2.5 DPIAs; and
8.2.6 records of data breaches.

8.3 We will conduct regular reviews of the personal information we process and update our documentation accordingly. This may include:

8.3.1 carrying out information audits to find out what personal information the AWSL holds;

8.3.2 distributing questionnaires and talking to members of AWSL to get a more complete picture of our processing activities; and

8.3.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

9 Privacy notice

9.1 The AWSL will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

10 Individual rights

10.1 You have the following rights in relation to your personal information:

10.1.1 to be informed about how, why and on what basis that information is processed—see the AWSL's Privacy Notice.

10.1.2 to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request;

10.1.3 to have data corrected if it is inaccurate or incomplete;

10.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

10.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and

10.1.6 to restrict the processing of personal information temporarily where you do not think it is accurate or where you have objected to the processing (we are considering whether the organisation's legitimate grounds override your interests).

10.2 If you wish to exercise any of the rights in paragraphs 10.1.3 to 10.1.6, please notify Linda Davies (see Clause 1.4) .

11 Information security

11.1 The AWSL will use appropriate technical and organisational measures in accordance with the AWSL's information retention and security policy to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

11.2 making sure that, where possible, personal information is pseudonymised or encrypted;

11.3 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

11.4 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

11.5 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

12 Storage and retention of personal information

12.1 Personal information will be kept securely in accordance with the AWSL's information and security policy.

12.2 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems (or put beyond use if this is not possible) and any hard copies will be destroyed securely.

13 Data breaches

13.1 A data breach may take many different forms, for example:

13.1.1 loss or theft of data or equipment on which personal information is stored;
13.1.2 unauthorised access to or use of personal information either by a member of staff or third party;
13.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;
13.1.4 human error, such as accidental deletion or alteration of data;
13.1.5 unforeseen circumstances, such as a fire or flood;
13.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
13.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

13.2 The AWSL will:

13.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if the breach is likely to result in a risk to the rights and freedoms of individuals; and
13.2.2 notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

14 International transfers

14.1 AWSL will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

15 Training

The AWSL will ensure that the Committee are adequately trained regarding their data protection responsibilities.