

## Privacy Notice and GDPR Compliance Statement

ASAP Computer Services are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Bill.

ASAP Computer Services are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation.

- **Information Audit** – we have carried out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.
- **Policies & Procedures**
  - **Data Protection** – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.
  - **Data Retention & Erasure** – Data will be retained based on Chapter 3, Article 17 (3e). “for the establishment, exercise or defence of legal claims”. This is because there may be future public liability issues arising from work carried out by ASAP. We acknowledge that clients have the ‘right to erasure’ but will need to agree to their waiving of any future public liability claims.
  - **Data Breaches** – We have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.
  - **International Data Transfers & Third-Party Disclosures** – In the event ASAP Computer Services stores data outside the UK it will only be in an encrypted and secure format.
  - **Subject Access Request (SAR)** – we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge.

- **Legal Basis for Processing** - we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.
- **Privacy Notice/Policy** – we have revised our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.
- **Obtaining Consent** - we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.
- **Data Protection Impact Assessments (DPIA)** – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).
- **Processor Agreements** – where we use any third-party to process personal information on our behalf, we will request proof of GDPR Compliance.
- **Special Categories Data** - where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition. Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

## **Data Subject Rights**

We provide easy to access information via our websites and a copy of this document.

Individuals have the following rights:

- Access on request to any personal information that ASAP Computer Services processes about them. This includes the purpose of the processing.
- We only collect personal information when we carry out work for customers and with their consent. This information will be retained based on Chapter 3, Article 17 (3e). “for the establishment, exercise or defence of legal claims”. This is because there may be future public liability issues arising from work carried out by ASAP.
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this.
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use.
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances.
- ASAP do not use any client information for direct marketing any contact will only be for business purposes.

## **Information Security & Technical and Organisational Measures**

ASAP Computer Services takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction. We have several layers of security measures including physical firewalling, enforced Antivirus and encryption of external devices.

## **GDPR Roles and Employees**

ASAP Computer Services have designated JamesShipman as our Data Protection Officer. He is responsible for promoting awareness of the GDPR across the organisation, identifying any gap areas and implementing the new policies, procedures and measures. ASAP Computer Services understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans.

If you have any questions about our preparation for the GDPR, please contact James Shipman on 0118 9845005.