General Data Protection Regulation (GDPR) Compliance Statement

Introduction

The ***EU General Data Protection Regulation ("GDPR")*** came into force across the European Union on 25th May 2018 and brought with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

Our Commitment

Staff Absence Management Limited herein referred to as SAM *('we' or 'us' or 'our')* 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 2018.

We 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. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

How we prepared for GDPR

SAM has a consistent level of data protection and security across our business.

Our preparation included: -

- ***Information Audit*** - carrying out a company-wide information audit to identify and assess what personal information we hold, where it came from, how and why it is processed, where it is stored and if and to whom it is disclosed.
- ***Policies & Procedures –*** We have revised our data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: -
    - ***Data Protection*** – our main policy and procedure document for data protection was 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*** – we updated our retention policy and schedule to ensure that we meet the *'data minimisation'* and *'storage limitation'* principles and that personal information is stored, archived and destroyed compliantly and ethically. We developed a dedicated erasure procedure in addition to our existing policies in place to meet the new *'Right to Erasure'* obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.
- ***Data Breaches*** – our breach procedures ensure that 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*** – where SAM stores or transfers personal information outside the EU, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information.
- ***Subject Access Request (SAR)*** – we revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply.

- ***Legal Basis for Processing*** - we reviewed 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 revised our Privacy Notice 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. A copy can be obtained at the following link - https://staffabsencemanagement.co.uk/privacy-policy/
- ***Obtaining Consent*** – we 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 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.
- ***Direct Marketing*** - we reviewed and revised the wording and processes for direct marketing, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.
- ***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 developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article

35 requirements. We 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). In addition to our DPIA's we also maintain a live Data Protection Risk Register, this enables any employee who identifies a potential data risk to document it quickly and effectively and speed up the process of establishing Control Measures to reduce identified risks further.

- ***Processor Agreements*** – where we use any third-party to process personal information on our behalf (*i.e. Payroll, Recruitment, Hosting etc*), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (*as well as we*), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.
- ***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.

The Types Of Data We Process

We have identified that we process the following types of personal data in providing our services to clients,

- Names of clients and clients employees
- Addresses
- Contact Details and Date of Birth
- Gender
- Information about contracts of employment, including start and end dates, role, location, working hours, holiday entitlement
- Salary information, Payroll Number and National Insurance Number
- Information relating to absence management cases including medical information
- Information relating to health and wellbeing
- Any other category of personal data which we may be notified of from time to time.

Data Subject Rights

In addition to the policies and procedures that ensure individuals can enforce their data protection rights, we provide easy to access information via our website, through induction and via our office, of an individual's right to access any personal information that SAM processes about them and to request information about: -

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source

- 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

Information Security and Technical and Organisational Measures

SAM 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 and have several layers of security measures, which include: -

- Information is encrypted with a two-layer authentication. We have moved to a secure cloud server so no data will be held directly on laptops, PC's or on the office based server. This will then be encrypted and securely backed up to protect information. All laptop's and PC's have also been encrypted.
- We are applying a forced password update every 90 days for internal systems, including Staff Absence Management Software
- Our websites hold SSL certification and have a backup provision included in order to be able to be restored quickly in the event of any disruptive activity, which is held securely and encrypted
- Our Accounts system is cloud-based and secure and can be accessed at any point from any location
- Archives have been located in a more secure storage area and we utilise a confidential shredding service
- Where possible staff work paper-free.

GDPR Roles and Employees

SAM have designated Ben Cain as our Data Protection Officer (DPO) to develop and implement our roadmap for complying with the new data protection regulation. He is responsible for promoting awareness of the GDPR across the business, assessing our GDPR compliance, identifying any gap areas and implementing the new policies, procedures and measures.

SAM 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. We delivered an employee training program specifically for GDPR as well as ongoing training and review it on a regular basis. Monthly Data Protection Audits will be carried out by our DPO in addition to regular reviews of all data security measures in place.

Information Management Accreditation

Whilst we do not currently hold ISO27001 status, we are striving to ensure that all the work we are doing to continue to keep data secure will enable us to achieve this status.

If you have any questions about our preparation for the GDPR, please contact Ben Cain at DPO@staffabsencemanagement.co.uk.

LAST UPDATED - July 2018