MARKS SATTIN

GDPR Policy

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the UK's Data Protection Act 1998. Its purpose is to protect the "rights and freedoms" of living individuals in relation to their personal data.

Policy Statement

The Board and management of Mark Sattin are committed to compliance with all relevant EU and UK laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information we collect and process in accordance with the General Data Protection Regulation (GDPR).

The GDPR and this policy apply to all of our personal data processing functions, including those performed on customers', clients', candidates', employees', and suppliers' personal data, and any other personal data we process from any source.

We have a designated Data Coordinator (DC) and is responsible for all data protection matters.

This policy applies to all employees (permanent and temporary), agency, and contract staff.

Any breach of the GDPR will be dealt with under our disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

Partner organisations and third parties working with or for us which have or may have access to personal data will be expected to adhere to all obligations imposed by data protection legislation. No third party may access personal data held by us without having first entered into a Data Sharing Agreement which imposes on the third party obligations no less onerous than those to which we are committed, and which gives us the right to audit compliance with the Agreement.

Definitions

The GDPR applies to the **processing of Personal Data** wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

The GDPR applies to all Data Controllers that are established in the European Union (EU) who process the personal data of Data Subjects. It also applies to Data Controllers outside of the EU who process personal data in order to offer goods and services to, or monitor the behaviour of, Data Subjects who are resident in the EU.

Personal Data – any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Sensitive Personal Data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a living person, data concerning health or data concerning a living person's sex life or sexual orientation.

Data Controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; where the purposes and means of such processing are determined by EU or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by EU or Member State law.

Data Subject – any living individual who is the subject of Personal Data held by an organisation.

Processing – any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed. The Data Controller is required to report Data Breaches to the Information Commissioner's Office (ICO), particularly breaches likely to adversely affect the Personal Data or privacy of the Data Subject.

Consent – means any freely given, specific, informed, and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data.

Third party – a natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, data processor and persons who, under the direct authority of the data controller or data processor, are authorised to process Personal Data.

Responsibilities and Roles

Marks Sattin is a Data Controller under the GDPR and is registered with the ICO under number Z9242448.

The Data Coordinator (DC) can be contacted at feedback@markssattin.com.

Senior Management and all those in managerial or supervisory roles throughout the organisation are responsible for developing and encouraging good information handling practices within the organisation; specific responsibilities are set out in individual job descriptions.

Our (DC) is (or reports to) a member of the senior management team and is directly accountable to the Board/Chief Executive for the management of personal data within our organisation and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes ensuring the development and implementation of all necessary processes and procedures, including security and risk management, to ensure compliance with the GDPR.

Our DC has specific responsibilities in respect of matters such as managing Subject Access Requests and is the first point of call for anyone seeking clarification on any aspect of data protection compliance within the organisation.

Compliance with data protection legislation is the responsibility of everyone in our organisation who processes personal data. Our Training Policy sets out specific training and awareness requirements in relation to specific roles and employees generally.

Employees are responsible for ensuring that any personal data about them and supplied by them to us is accurate and up-to-date.

Our DC will ensure that an annual review of data protection compliance is carried out by our auditors.

Data Protection Principles

All processing of personal data must be conducted in accordance with the Data Protection Principles as set out in the GDPR and outlined below. Our policies and procedures are designed to ensure compliance with these Principles.

Principle 1

Personal data must be processed lawfully, fairly, and transparently

Lawful – we need to identify a lawful basis before we can process personal data, for example, legitimate interest.
Fairly – in order for processing to be fair, we have to make certain information available to Data Subjects. This applies whether the Personal Data was obtained directly from Data Subjects or from other sources.
Transparently – the GDPR includes rules on giving privacy information to Data Subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the Data Subject in an intelligible form using clear and plain language.

Principle 2

Personal Data can only be collected for specific, explicit, and legitimate purposes

The data we obtain for specified purposes must not be used for a purpose that is incompatible with those formally notified to the ICO as part of our GDPR register of processing.

Principle 3

Personal Data must be adequate, relevant, and limited to what is necessary for processing

We cannot collect information that is not strictly necessary for the purpose for which it is obtained.

Principle 4

Personal Data must be accurate and, where necessary, kept up to date.

Every reasonable step must be taken to ensure that Personal Data that are inaccurate are erased or rectified without delay data that is stored by us must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

Principle 5

Personal Data must be kept in a form such that the Data Subject can be identified only as long as is necessary for processing.

We should only retain Personal Data for as long as we need it.

Principle 6

Personal Data must be 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

Demonstrating Accountability

The GDPR includes provisions that promote Accountability and Governance. These complement the GDPR's transparency requirements. Accountability requires us to demonstrate that we comply with the GDPR Principles.

We will demonstrate compliance with the GDPR Principles by implementing and adhering to data protection policies, implementing technical and organisational measures, as well as adopting techniques such as Data Protection by Design, Data Protection Impact Assessments, breach notification procedures and incident response plans.

Data Subjects' Rights

The GDPR provides the following rights for individuals in relation to their personal data:

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.

Data Subjects may make Subject Access Requests relating to their Personal Data. Our Subject Access Request Policy describes how we will ensure that our response to the request complies with the requirements of the GDPR.

Our DC is responsible for responding to requests for information from Data Subjects within one calendar month in accordance with our Subject Access Request Policy. This can be extended to two months for complex requests in certain circumstances. If we decide not to comply with the request, the DC must respond to the Data Subject to explain our reasoning and inform them of their right to complain to the ICO and seek judicial remedy.

Data Subjects have the right to complain to us about the processing of their Personal Data, the handling of a Subject Access Request and to appeal against how their complaints have been handled.

Consent

We understand 'consent' to mean that it has been explicitly and freely given, and it is a specific, informed and unambiguous indication of the Data Subject's wish that, by statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her. The Data Subject can withdraw their consent at any time.

We also understand 'consent' to mean that the Data Subject has been fully informed of the intended processing and has signified their agreement while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.
Consent cannot be inferred from non-response to a communication. As Data Controller, we must be able to demonstrate that consent, where necessary, was obtained for the processing operation.

For Sensitive Personal Data, explicit written consent of Data Subjects must be obtained unless an alternative legitimate basis for processing exists.

Collection of Data

All data collection forms (electronic and paper-based), including data collection requirements in new information systems, must include a fair processing statement or a link to our Privacy Policy.

Accuracy of Data

Our DC is responsible for ensuring that all employees are trained in the importance of collecting accurate data and maintaining it.

Employees are required to notify the Human Resources department of any changes in their personal circumstance's which may require personal records be updated accordingly.

Our DC is responsible for ensuring that appropriate procedures are in place to keep Personal Data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

Security of Data

All Personal Data should be accessible only to those who need to use it. All Personal Data should be treated with the highest security as set out in our Data Security Policy.

No less than annually our DC will carry out a risk assessment taking into account all the circumstances of our data controlling and processing operations.

In determining appropriateness of all technical and organisational security measures, the DC will consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers, candidates and clients) if a security breach occurs, the effect of any security breach on our organisation itself, and any likely reputational damage, including the possible loss of customer trust.

It is strictly prohibited to remove Personal Data from our premises for any reason other than carrying out legitimate processing activities.

Processing of Personal Data 'off-site' presents a potentially greater risk of loss, theft, or damage to Personal Data and the precautions that **must** be taken are set out in our Data Security Policy.

All employees are responsible for ensuring that any Personal Data that we hold and for which they are responsible is kept securely and is not, under any condition, disclosed to any third party unless that third party has been specifically authorised by us to receive that information and has entered into a Data Sharing Agreement.

Disclosure of Data

All requests to provide Personal Data must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Coordinator.

We must ensure that Personal Data is not disclosed to unauthorised third parties, which includes family members, friends, government bodies, and, in certain circumstances, the police. All employees should exercise caution when asked to disclose Personal Data held on another individual to a third party.

Retention and Disposal of Data

We shall not keep Personal Data in a form that permits identification of Data Subjects for a longer period than is necessary in relation to the purpose(s) for which the data was originally collected.

The retention period for each category of Personal Data is set out in our Retention and Disposal Policy. Personal Data will be retained in line with our Retention and Disposal Policy and, once its retention date is passed, it must be securely destroyed as set out in this policy.

On at least an annual basis, our DC will review the retention dates of all the Personal Data processed by our organisation and will identify any data that is no longer required. This data will be securely archived, deleted or destroyed in line with our Retention and Disposal Policy.

Our DC must specifically approve any data retention that exceeds the retention periods defined in our Retention and Disposal Policy, and must ensure that the justification is clearly identified and recorded.

We may store data for longer periods if the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the Data Subject. Any such retention must be approved in advance by the DC.

International Data Transfers

Under GDPR transfers of Personal Data outside of the European Economic Area can only be made if specific safeguards exist.

If we transfer data outside the EEA we satisfy ourselves that the conditions laid down in the Regulation are complied with by the controller and processor by:

1. **An adequacy decision, or**
2. **Privacy Shield, or**
3. **Binding corporate rules, or**
4. **Model contract clauses, or**
5. **Exceptions**
    - the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the Data Subject due to the absence of an adequacy decision and appropriate safeguards;
    - the transfer is necessary for the performance of a contract between the Data Subject and the controller or the implementation of pre-contractual measures taken at the Data Subject's request;
    - the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the controller and another natural or legal person;
    - the transfer is necessary for important reasons of public interest;
    - the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
    - the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

Data Processed Register

We have established a Data Processed Register that records:

- each type of Personal Data;
- why it is collected;
- the lawful grounds for processing;
- where it is held;
- the Responsible Person for the data;
- its Review Date; and
- how it is kept accurate.

Data Protection Impact Assessments (DPIA)

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of living peoples, we shall, prior to the processing, carry out a Data Protection Impact Assessment of the envisaged processing operations. All DPIAs should lead by or overseen by the DC.

Where, as a result of a DPIA it is clear that we are about to commence processing of Personal Data that could cause damage and/or distress to the Data Subjects, the decision as to whether or not we may proceed must be referred to senior management for approval to proceed.

Our DC shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, refer to the ICO for guidance and advice.