EMSCognito Competitive Edge Consulting	**08-08_EMS Cognito Data Protection Policy V1.2**	**Written**	MG
		Approved	RK
		Date	18-Mar-19
		Review	18-Mar-22

Change Summary
Updated to new template

Roles and Responsibilities
All EMS Cognito Policies are to be read and understood by all staff.

Policy Statement

EMS Cognito is committed to adopting best practice in protecting the personal information of all candidates, employees, and partner and supplier organisations. This policy sets out EMS Cognito's approach to comply with legal requirements and maintain the confidence of those individuals who trust EMS Cognito with their personal information.

Why do we need this Policy?

The purpose of the Data Protection Act 2018 is to protect individuals from having their personal data or privacy exploited or abused. This places the onus on organisations and individuals processing such data to ensure that the processing is conducted in a fair, lawful and secure way. It is therefore of vital importance that all EMS Cognito's employees, and contract workers comply with the requirements of the Act.

What/who does the policy apply to?

This policy applies to all:

- employees
- contract workers

As a public body, the Act applies to all recorded information about living individuals held by EMS Cognito. This includes (but is not limited to) information about:

- employees and ex-employees (or contract workers) of EMS Cognito
- candidates

The Act applies equally to images (e.g. photos or CCTV footage) or recorded audio information that allows individuals to be identified, as to written information. One person's opinion about another individual is personal information about both of them. It applies whether the individual is located in the UK, European Economic 2 Area or worldwide

What is affected?

The Act applies to any 'processing' of personal information. This is defined very widely and includes gathering, holding, analysing or using, sharing with others, moving, deleting or shredding.

Particularly stringent requirements apply to processing of 'sensitive personal data' defined in the Act as information relating to:

- racial or ethnic origin
- political opinions

- religious or other similar beliefs
- trade union membership
- physical or mental health
- sexual life
- criminal offences or proceedings

Extra care should also be taken when processing information about individuals where a duty of confidence might apply.

What support is available to help EMS Cognito implement this policy?

Information Commissioner's Office website http://www.ico.gov.uk

Further information

1 Processing purposes

The Act requires EMS Cognito to specify the reason(s) for processing any personal information. We will use personal information collected for the following purposes:

- staff administration
- advertising, marketing and public relations
- accounts and records
- education
- licensing and registration
- the consideration of complaints

2 Obligations on EMS Cognito and its employees and contract workers

There are eight Principles included in the Act. These Principles are obligations that EMS Cognito must follow in any processing of personal information. These apply equally to EMS Cognito employees and contracted workers. EMS Cognito must also ensure that any suppliers (including individual consultants) comply with these Principles in their work for EMS Cognito. The Principles are summarised below:

2.1 Personal data shall be processed fairly and lawfully, meaning:

- The processing must be generally fair and reasonable.
- Individuals must be told why EMS Cognito needs any personal information that is being gathered, including the reason for any intention to share it with others.
- The processing must not breach a confidence unless the individual has agreed, or it is required by law or it is in the greater public interest (e.g. whistleblowing).
- Personal information should only be accepted from sources that are lawfully allowed to supply it.
- The processing must not go beyond EMS Cognito's statutory powers.
- EMS Cognito cannot process any personal information unless one of the following conditions applies:
  - Individuals have freely given fully informed consent.
  - It is necessary for a contract with the individual or other legal obligation.
  - It will keep the individual alive.

- It is required by a statutory obligation.
- It is necessary for the legitimate interests of EMS Cognito or another, and doesn't prejudice the individual's legitimate interests.

EMS Cognito cannot process any 'sensitive personal data' unless an additional more stringent set of conditions has been satisfied.

2.2 Personal data shall be obtained for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose, meaning:

- Any further processing must be compatible with the original purpose for which the data was obtained.

2.3 Personal data shall be adequate, relevant and not excessive in relation to that purpose, meaning:

- Enough personal information must be obtained to allow EMS Cognito to fulfil the purpose for gathering it (e.g. it must be possible to distinguish between two similar records).
- Extra items of personal information should not be collected on the basis that they might be useful for some unspecified purpose in the future.
- Where particular information is needed for a subset of individuals, but not everyone, it should only be requested for the particular subset.

2.4 Personal data shall be accurate and kept up to date, meaning:

- Reasonable steps should be taken to keep personal information up to date.
- Reasonable steps should be taken to ensure that personal information is accurate.
- Any inaccuracies (including those where the individual points out an inaccuracy) should be promptly corrected.

2.5 Personal data shall not be kept for any longer than is necessary for that purpose, meaning:

- Team retention schedules should be consistently applied.
- Personal information should be destroyed (e.g. deleted or shredded) securely.

2.6 Personal data shall be processed in accordance with individuals' rights, meaning:

- EMS Cognito must ensure that its systems, processes, policies and practices are designed to accommodate individuals' option to exercise their rights.
- One important right is the individual's right to access personal information held about them. Good information management practice will ensure that all personal information about an individual can be easily located.
- Any reference to individuals in e-mails or correspondence, including any expression of opinion or intention about them, is covered by the Act.
- Appropriate care should be taken to express such opinions or intentions in a professional manner.

2.7 Appropriate technical and organisational measures shall be taken to protect personal data, meaning:

- Personal information must be stored or sent to others in a secure manner, whether on computer or paper, internally or externally.
- The sensitivity and risk level for personal information used within a business area should be considered, and particularly stringent security controls put in place for confidential or 'sensitive' personal information.
- EMS Cognito must ensure that its employees and contract workers using personal information (and any staff working for suppliers using personal information for which EMS Cognito is responsible) are reliable through vetting, training, monitoring or supervision.
- Colleagues and/or suppliers (including individuals) should be provided with access to personal data only as required in relation to the purpose for which it was obtained. Ensure that they are aware of their responsibilities set out in this policy and any related policies, and of the degree of access to personal information that is authorised for the purpose of their role.
- Disclose the data only to those who require it in relation to the purpose for which it was obtained. Any sharing of personal data must comply with the ICO's statutory code of practice on data sharing, which sets out mandatory requirements to ensure that data is shared in a way that is fair and in line with individuals' rights and expectations.
- When disclosing personal information to the individual or anyone else, take reasonable steps to confirm their identity. Be alert to the possibility of individuals attempting to obtain personal information by deception.
- Regardless of contract value, particular requirements apply to the selection of suppliers who will use personal information on EMS Cognito's behalf (e.g. printers, couriers, software suppliers testing with real individual records, development consultants holding contact details for appointees).

2.8 Personal data shall not be transferred outside the European Economic Area (EEA) unless an adequate level of data protection is in place, meaning:

- A need may arise for EMS Cognito to transfer personal information outside the EEA for various reasons, e.g. where a supplier's equipment (such as a server) is based outside the EEA, or when exchanging information about consultants working in international markets, or information about candidates or staff based in international centres.
- The Act provides that this transfer can legitimately take place where all of the other Principles have been satisfied

3 Individuals' rights

The Act gives a number of rights to individuals and EMS Cognito must ensure that its systems, processes, policies and practices are designed to enable individuals to exercise these rights.

3.1 Right to access personal information held about them

- EMS Cognito will log and co-ordinate the response to any requests for personal information from individuals which are outside the usual run of business. Individuals requesting access to

such information will be made aware of the process, fee and statutory deadline that apply to these requests.

- Individuals may authorise a third party representative to act on their behalf when requesting their personal information. This could be a solicitor, carer or family member. In this case, EMS Cognito must be satisfied that the representative is entitled to make the request on behalf of the individual. It is the individual's responsibility to provide evidence that they have authorised the representative to make the request on their behalf.
- The right extends to include any archived information or information which has been deleted but can still be retrieved, e.g. held in e-mail trash.

3.2 Right to object to direct marketing

- Where an individual notifies EMS Cognito in writing that they wish to object to direct marketing, their details should be suppressed (not deleted) and no further direct marketing activity should take place.

3.3 Right to object to processing

- Individuals have a limited right to object in writing to processing which is likely to cause substantial unwarranted damage or distress in particular circumstances.

3.4 Right to object to automated decision-making

- Individuals have a limited right to object in writing to any decision-making which significantly affects them and which is solely taken by automated means.
- Where automated decision-making is planned, safeguards must be in place to protect individuals' rights in the event of a negative outcome, e.g. prior quality assurance or an appeal mechanism.

4 Data sharing and disclosures

EMS Cognito will share personal data with partner organisations where this is necessary in relation to the purpose for which the data was obtained, and in line with its notification (e.g. SQA). Personal information will not be passed on to any third party companies for marketing purposes

5 Roles and responsibilities

5.1 Employees and contract workers

Individuals are responsible for ensuring that they understand and comply with the implications of the Act and this policy in relation to their role. They are also responsible for adhering to good information management practice.

5.2 Management

EMS Cognito management is responsible for ensuring that access to personal information is given to employees and contract workers in accordance with their duties. They are also responsible for ensuring that employees and contract workers are aware of their responsibilities set out in this policy (and any related policies) and of the degree of access to personal information that is

authorised for the purpose of their role. They are also responsible for handling any actual or potential data protection breaches.

6 Security incident reporting

If a member of staff and contract worker becomes aware of an actual or potential breach of security in relation to personal information, they should report it immediately to management. Quick action can be crucial in mitigating the negative effects of a breach.

7 Protecting personal information

EMS Cognito must continually ensure that its collection, storage and use of personal data comply with its obligations in the Data Protection Act. It is the responsibility of every member of staff and contract workers to uphold these responsibilities, treating all individuals' personal information with the same respect that they would expect for their own.

9 Glossary

The following key concepts are important in understanding this policy:

Personal data is information held about living, identifiable individuals including expressions of opinion or intention about them.

Processing includes obtaining, recording or using the personal data — anything from getting it, moving it, analysing it, sharing it with anyone, deleting or destroying it.

Data controller refers to an organisation or individual who decides the purpose and manner in which personal data should be processed.

Data processor is a person or organisation who processes personal data on behalf of a data controller, eg printer, courier, software development contractor.

Data subjects are living people about whom the personal data is held.

Data subject access request is a written request from a data subject (or an authorised third party) for access to personal data about them processed by EMS Cognito.
Sensitive personal data means personal data that relates to:

- racial or ethnic origin
- political opinions
- religious or similar beliefs
- trade union membership status
- physical or mental health or condition
- sexual life
- commission or alleged commission of any offence
- proceedings or sentence for any alleged offence