GEM Partnership Ltd
Data Protection Policy

1. Responsibility

1.1 The Data and Compliance Team responsible for this policy are;

1.1.1 Annie Dorner – Compliance & Projects Manager

1.1.2 James Proudlock – Digital & Data Manager

2. Introduction

2.1 All organisations that process personal data are required to comply with data protection legislation. This includes in particular the Data Protection Act 2018 (or its successor) and the UK General Data Protection Regulation (together the 'Data Protection Laws'). The Data Protection Laws give individuals (known as 'data subjects') certain rights over their personal data whilst imposing certain obligations on the organisations that process their data.

2.2 As a recruitment and training business GEM Partnership collects and processes both personal data and sensitive personal data. It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

2.3 This policy sets out how GEM Partnership implements the Data Protection Laws. It should be read in conjunction with the Data Protection Procedure.

3. Definitions

3.1 In this policy the following terms have the following meanings:

3.1.1 '**Consent**' means any freely given, specific, informed and unambiguous indication of an individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of persona data relating to him or her;

3.1.2 '**Data controller**' means an individual or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data;

3.1.3 '**Data processor**' means an individual or organisation which processes personal data on behalf of the data controller;

3.1.4 '**Personal data**' means any information relating to an individual who can be identified, such as by 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.

3.1.5 '**Personal data breach**' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;

3.1.6 '**Processing**' means any operation or set of operations performed on personal data, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.1.7 '**Profiling**' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that natural person's performance at work, economic

situation, health, personal preferences, interests, reliability, behaviour, location or movements;

3.1.8 **'Pseudonymisation'** means the processing of personal data in such a manner that the personal data can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;

3.1.9 **'Sensitive personal data'** means 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, data concerning health, an individual's sex life or sexual orientation and an individual's criminal convictions.

3.1.10 **'Supervisory authority'** means an independent public authority which is responsible for monitoring the application of data protection. In the UK the supervisory authority is the Information Commissioner's Office (ICO).

4. Data processing under the Data Protection Laws.

4.1 GEM Partnership processes personal data in relation to its own staff, work-seekers, learners, apprentices, individual client contacts and is a data controller for the purposes of the Data Protection Laws. GEM Partnership has registered with the ICO and its registration number is Z2079409.

4.2 GEM Partnership may hold personal data on individuals for the following purposes:

4.2.1 Staff administration;

4.2.2 Advertising, marketing and public relations.

4.2.3 Accounts and records;

4.2.4 Administration and processing of work-seekers' personal data for the purposes of providing work-finding services, including processing using software solution providers and back-office support'

4.2.5 Administration and processing of learner, apprentice or delegate personal data for the purposes of providing education and training.

4.2.6 Administration and processing of clients' personal data for the purposes of supplying/introducing work-seekers, apprentices or learners.

4.2.7 Administration and processing of apprentice or learner personal data for the provision of complying with funding rules, Department for Education (DfE) and the Education and Skills Funding Agency (ESFA).

4.3 The data protection principles. The Data Protection Laws require GEM Partnership acting as either data controller or data processor to process data in accordance with the principles of data protection. These require that personal data is:

4.3.1 Processed lawfully, fairly and in a transparent manner;

4.3.2 Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

4.3.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4.4 Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

4.5 Kept for no longer than is necessary for the purposes for which the personal data are processed;

4.6 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; and that

4.6.1 The data controller shall be responsible for, and be able to demonstrate, compliance with the principles.

5. Legal basis for processing

5.1 GEM Partnership will only process personal data where it has a legal basis for doing so. Where GEM Partnership does not have a legal reason for processing personal data any processing will be a breach of the Data Protection Laws.

5.2 GEM Partnership will review the personal data it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date.

5.3 Before transferring personal data to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back-office support), GEM Partnership will establish that it has a legal reason for making the transfer.

6. Privacy by design and by default

6.1 GEM Partnership has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all processing activities. This includes implementing measures such as:

6.1.1 Data minimisation (i.e. not keeping data for longer than is necessary);

6.1.2 Pseudonymisation;

6.1.3 Anonymization.

6.1.4 Cyber security.

7. Rights of the individual

7.1 GEM Partnership shall provide any information relating to data processing to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. GEM Partnership may provide this information orally if requested to do so by the individual.

7.2 Privacy notices.

7.2.1 Where GEM Partnership collects personal data from the individual, GEM Partnership will give the individual a privacy notice at the time when it first obtains the personal data or soon thereafter as part of a handbook. Privacy notices are available to view on the company website and also as a link within all employee email footers and email correspondence.

7.2.2 Where GEM Partnership collects personal data other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the personal data, but at the latest within one month. If GEM Partnership intends to disclose the personal data to a third party then the privacy notice will be issued when the personal data are first disclosed (if not issued sooner).

7.2.3 Where GEM Partnership intends to further process the personal data for a purpose other than that for which the data was initially collected, GEM Partnership will give the individual information on that other purpose and any relevant further information before it does the further processing.

7.3 Subject access requests.

7.3.1 The individual is entitled to access their personal data on request from the data controller. Subject Access Request procedure can be found in the Subject Access Request Policy & Procedure.

7.4 Rectification The individual or another data controller at the individual's request, has the right to ask GEM Partnership to rectify any inaccurate or incomplete personal data concerning an individual.

7.4.1 If GEM Partnership has given the personal data to any third parties it will tell those third parties that it has received a request to rectify the personal data unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however GEM Partnership will not be in a position to audit those third parties to ensure that the rectification has occurred. The procedure to Process this request can be found in the Subject Access Request Policy.

7.5 Erasure The individual or another data controller at the individual's request, has the right to ask GEM Partnership to erase an individual's personal data.

7.5.1 If GEM Partnership receives a request to erase it will ask the individual if s/he wants his personal data to be removed entirely or whether s/he is happy for his or her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). GEM Partnership cannot keep a record of individuals whose data it has erased so the individual may be contacted again by GEM Partnership should GEM Partnership come into possession of the individual's personal data at a later date.

7.5.2 If GEM Partnership has made the data public, it shall take reasonable steps to inform other data controllers and data processors processing the personal data to erase the personal data, taking into account available technology and the cost of implementation.

7.5.3 If GEM Partnership has given the personal data to any third parties it will tell those third parties that it has received a request to erase the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however GEM Partnership will not be in a position to audit those third parties to ensure that the rectification has occurred.

7.6 Restriction of processing. The individual or a data controller at the individual's request, has the right to ask GEM Partnership to restrict its processing of an individual's personal data where:

7.6.1 The individual challenges the accuracy of the personal data;

7.6.2 The processing is unlawful and the individual opposes its erasure;

7.6.3 GEM Partnership no longer needs the personal data for the purposes of the processing, but the personal data is required for the establishment, exercise or defence of legal claims; or

7.6.4 The individual has objected to processing (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of GEM Partnership override those of the individual.

7.7 If GEM Partnership has given the personal data to any third parties it will tell those third parties that it has received a request to restrict the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold - however GEM Partnership will not be in a position to audit those third parties to ensure that the rectification has occurred.

7.8 Data portability. The individual shall have the right to receive personal data concerning him or her, which he or she has provided to GEM Partnership, in a structured, commonly used and machine-readable format and have the right to transmit those data to another data controller in circumstances where:

7.8.1 The processing is based on the individual's consent or a contract

7.8.2 The processing is carried out by automated means. Where feasible, GEM Partnership will send the personal data to a named third party on the individual's request.

7.9 Object to processing. The individual has the right to object to their personal data being processed based on a public interest or a legitimate interest. The individual will also be able to object to the profiling of their data based on a public interest or a legitimate interest.

7.10 GEM Partnership shall cease processing unless it has compelling legitimate grounds to continue to process the personal data which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

7.11 The individual has the right to object to their personal data for direct marketing. Please refer to GEM Partnership's Social Media Staying Safe Online Cyber Bullying Policy for further information.

7.12 Enforcement of rights. All requests regarding individual rights should be sent to the Data and Compliance Team.

7.13 GEM Partnership shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision-making processes or profiling within 1 month of receipt of the request. GEM Partnership may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

7.14 Where GEM Partnership considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature GEM Partnership may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

7.15 Automated decision-making GEM Partnership will not subject individuals to decisions based on automated processing that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

7.15.1 Is necessary for the entering into or performance of a contract between the data controller and the individual;

7.15.2 Is authorised by law; or

7.15.3 The individual has given their explicit consent.

7.16 GEM Partnership will not carry out any automated decision-making or profiling using the personal data of a child.

8. Personal data breaches

8.1 All data breaches should be referred to a member of the Data and Compliance Team(see point 1).

8.2 Personal data breaches where GEM Partnership is the data controller:

8.2.1 Where GEM Partnership establishes that a personal data breach has taken place, GEM Partnership will take steps to contain and recover the breach. Where a personal data breach is likely to result in a risk to the rights and freedoms of any individual GEM Partnership will notify the ICO.

8.2.2 Where the personal data breach happens outside the UK, GEM Partnership shall alert the relevant supervisory authority for data breaches in the effected jurisdiction.

8.3 Personal data breaches where GEM Partnership is the data processor:

8.3.1 GEM Partnership will alert the relevant data controller as to the personal data breach as soon as they are aware of the breach.

8.4 Communicating personal data breaches to individuals:

8.4.1 Where GEM Partnership has identified a personal data breach resulting in a high risk to the rights and freedoms of any individual, GEM Partnership shall tell all affected individuals without undue delay.

8.4.2 GEM Partnership will not be required to tell individuals about the personal data breach where:

8.4.2.1 GEM Partnership has implemented appropriate technical and organisational protection measures to the personal data affected by the breach, in particular to make the personal data unintelligible to any person who is not authorised to access it, such as encryption.

8.4.2.2 GEM Partnership has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialize.

8.4.2.3 It would involve disproportionate effort to tell all affected individuals. Instead, GEM Partnership shall make a public communication or similar measure to tell all affected individuals.

9. The Human Rights Act 1998

9.1 All individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with personal data these should be respected at all times:

9.1.1 Right to respect for private and family life.

9.1.2 Freedom of thought, belief and religion.

9.1.3 Freedom of expression.

9.1.4 Freedom of assembly and association.

9.1.5 Protection from discrimination in respect of rights and freedoms under the HRA

10. Complaints

10.1 If you have a complaint or suggestion about GEM Partnership's handling of personal data then please contact a member of the Data and Compliance Team.

10.2 Alternatively you can contact the ICO directly on 0303 123 1113 or at https://ico.org.uk/global/contact-us/email/

GEM Partnership Ltd
Data Protection Procedure

1. Responsibility

1.1. The Data and Compliance Team responsible for this policy are;

1.1.1. Annie Dorner – Compliance & Projects Manager

1.1.2. James Proudlock – Digital & Data Manager

2. Information Security

2.1. All Company staff are responsible for notifying a member of the Data and Compliance Team where information is known to be old, inaccurate or out of date or a request for erasure, access, rectification or restriction of processing has been received from the individual. Company staff are also responsible for notifying those listed above where any request for data portability, objection to processing or where consent to process has been withdrawn and has been received from the individual.

2.2. The incorrect processing of personal data e.g. sending an individual's details to the wrong person, allowing unauthorised persons access to personal data, sending information out for purposes for which the individual did not give their consent, or not having a lawful reason to process personal data, may give rise to a breach of contract and/or negligence leading to a claim against GEM Partnership for damages from an employee, work-seeker, apprentice, learner, funding partner or client contact.

2.3. In addition all Company staff should ensure that adequate security measures are in place to limit the risk of personal data breaches. For example:

2.3.1. Staff should lock their computer screens when they are not in use and auto lock should be enabled to lock automatically after 10 minutes of inactivity.

2.3.2. All devices, whether company or personal devices (including but not limited to computers, mobile phones, tablets or other hand-held devices) containing personal data relating to the services of GEM Partnership shall be encrypted and password protected. OR All personal data collected via a company or personal device for the purposes of providing GEM Partnership's services, should be processed through GEM Partnership's CRM which is password protected.

2.3.3. Staff should not disclose their passwords to anyone.

2.3.4. Email should be used with care. Company staff must ensure that emails are sent only to the intended recipient/s. Where Company staff send an email in error then the email must be recalled immediately and Company staff must inform a member of the Data and Compliance Team of the error so that any risk of a personal data breach can be limited.

2.3.5. Personnel files and other personal data for internal staff should be stored securely either in secure storage in Peterlee Office (for historic data) OR on Sharepoint in a secured folder only

accessible to relevant personnel to prevent unauthorised access. They should not be removed from their usual place of storage without good reason.

2.3.6. Personnel files and any other personal data in relation to workseekers or temporary workers, should be stored securely on CRM system, Chameleoni or Sharepoint only. Data may be stored temporarily on Jotform, User Outlook account, Mobile Devices but should be moved to either Chamleoni or Sharepoint (as appropriate) immediately and then deleted from other locations.

2.3.7. Learner files (apprenticeships, adult skills funding & commercial) should always be stored securely on either PICS, GEM Sharepoint, secure archiving at GEM site, Individual Learner Record (.gov), awarding body portals (Highfield, UCE, City & Guilds, ILM, EAL, QualTrain, TQUK, DSW, Ace360) or BKSB.

2.4. Personal data and special category data should only be stored for the periods set out in GEM Partnership's data retention policy.

2.5. Processing includes the destruction or disposal of personal data. Therefore, staff should take care to destroy or dispose of personal data safely and securely, whether this is electronic or paper based. Paper based material should be shredded or stored as confidential waste awaiting safe destruction.

2.5.1. The process is "Action and Store or Delete" when processing data, take the appropriate action as defined by internal processes to store the data securely in an approved location if required and/or delete from any non-approved locations immediately.

2.5.2. Compliance Managers are responsible for identifying any records and removing data from ALL systems in line with data retention policy on a minimum of Annual basis.

2.5.3. Chameleoni process for workseekers/temporary workers data;

2.5.3.1. Any candidate records will be subject to a request to GDPR "opt in" every 2 years of being on the system. This is an automated process through the system.

2.5.3.2. Compliance Manager will run a report monthly for any candidates who have decided to GDPR "opt out", check when they last worked for the organization and remove their data from the database if they have not worked in the last 6 years (legal requirements for data retention). If they have worked in the last 6 years, all contact details will be removed, record set to archive and a note added for when the record can be deleted.

2.5.3.3. Compliance Manager will run a report every 6 months for any candidate records tagged as GDPR "No Response" (they have received the GDPR request to opt in/out and have not responded), these candidates will receive a "reminder" email and then if no response again within 1 week they will;

2.5.3.3.1. If they have worked in the last 6 years they will have all contact details removed, record set to archive and a note added for earliest deletion date, OR;

2.5.3.3.2. Be removed from the database if they have not worked in the last 6 years

2.5.4. Jotform process for learners, apprentices, delegates, workseekers & temporary workers data;

2.5.4.1. All data, documents should be extracted from the system and actioned/stored as required in line with data retention policy and then set to auto delete from Jotform after 90 days.

2.5.5. Sharepoint process for learners, apprentices & delegates data;

2.5.5.1. Documents should be uploaded to secure folder and titled with the individuals name and completion date. Monthly review by Compliance Manager to review data in line with data retention policy and delete if required.

2.5.6. PICS process for learners, apprentices & delegates data;

2.5.6.1. Monthly review by Compliance Manager to review data in line with data retention policy and delete if required.

3. Rights of the Individual.

3.1. An individual has the following rights under the Data Protection Laws:

3.1.1. The right to be informed of what information GEM Partnership holds on them – this is typically given to the individual in a privacy notice;

3.1.2. The right of access to any personal data that GEM Partnership holds on them – this is usually referred to as a 'subject access request';

3.1.3. The right to rectification of personal data that the individual believes is either inaccurate or incomplete;

3.1.4. The right to erasure of their personal data in certain circumstances;

3.1.5. The right to restrict processing of their personal data;

3.1.6. The right to data portability of their personal data in specific circumstances;

3.1.7. The right to object to the processing of their personal data where it is based on either a legitimate interest or a public interest;

3.1.8. The right not to be subjected to automated decision making and profiling; and

3.1.9. The right to withdraw consent where it was relied upon to process their personal data.

3.1.10. The right to be informed Any individual whose personal data is processed by GEM Partnership will have the right to be informed about such processing. They will have the right to be informed about who, what, where and why the data is processed. This information should be delivered in a privacy notice, in writing and where appropriate electronically. Depending on where the personal data are being collected, an individual may be directed to GEM Partnership's website privacy notice or be given a copy of a privacy notice. This privacy notice should be issued in instances where either:

3.1.10.1. GEM Partnership collects/processes data directly from the individual; or

3.1.10.2. GEM Partnership has not collected/processed the data from the individual directly.

3.2. In addition:

3.2.1. Where personal data has been collected from the individual the privacy notice will need to be issued at the point the data is collected or soon thereafter as part of a handbook. Privacy notices are available to view on the company website and also as a link within all employee email footers and email correspondence.. Where GEM Partnership intends to further process the personal data for a purpose other than that for which the personal data was collected, GEM Partnership shall provide the individual, prior to that further processing, with information on that other purpose and with any relevant further information in [a new/an] updated privacy notice.

3.2.2. Where personal data has not been obtained from the individual, GEM Partnership shall provide the privacy notice within a reasonable period after obtaining the personal data, but at the

latest within one month, having regard to the specific circumstances in which the personal data are processed. If the personal data are to be used to communicate with the individual then the privacy notice will be issued at the time of the first communication with the individual. If a disclosure to another recipient is envisaged, then the privacy notice will be issued to the individual at the latest when the personal data are first disclosed.

3.3. Company staff will be responsible for issuing privacy notices to individuals whose personal data is processed by GEM Partnership in the timeframes and circumstances mentioned above.

	Where GEM Partnership collects data from the individual:	Where personal data has not been obtained from the individual:
The identity and contact details of GEM Partnership and where applicable the controller's representatives and/or data protection officer.	Yes (Y)	Y
The purposes of processing and the legal basis for the processing.	Y	Y
The legitimate interest of the data controller or third party, where applicable.	Y	Y
The categories of personal data.	No (N)	Y
Recipients or categories of recipients of personal data.	Y	Y
Details of transfers to third parties or countries and the safeguards in place.	Y	Y
The retention period of the data or the criteria used to determine the retention period.	Y	Y
The existence of individual's rights including the right of access, rectification, erasure, restriction of processing, objection to processing and the right to data portability.	Y	Y
The existence of the right to withdraw consent where it has been given and relied upon.	Y	Y
The right to lodge a complaint with the Information Commissioner's Office or any other relevant supervisory authority.	Y	Y
The source the personal data originates from and whether it came from publicly accessible sources.	N	Y

	Where GEM Partnership collects data from the individual:	Where personal data has not been obtained from the individual:
Whether the provision of personal data form part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data.	Y	N
The existence of automated decision-making, including profiling and information about how decisions are made, the significance and the consequences.	Y	Y

Table 1: Privacy information to be given to the individual

4. The Right to Access ('Subject Access Request')

4.1. Individuals are entitled to obtain access to their personal data on request, free of charge except in certain circumstances.

4.2. An individual will be entitled to the following information:

4.2.1. Confirmation that their personal data is or is not being processed;

4.2.2. Access to the personal data undergoing processing;

4.2.3. The purposes of the processing;

4.2.4. The categories of personal data concerned;

4.2.5. The recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

4.2.6. Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

4.2.7. The existence of the right to request from GEM Partnership rectification or erasure of personal data or restriction of processing of personal data concerning the individual or to object to such processing;

4.2.8. The right to lodge a complaint with the ICO or any other relevant supervisory authority;

4.2.9. Where the personal data are not collected from an individual, any available information as to the source of that information;

4.2.10. The existence of automated decision-making, including profiling, based on a public interest or a legitimate interest and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

4.3. If GEM Partnership transfers the individual's personal data to a third country or to an international organisation, the individual shall have the right to be informed of the appropriate safeguards in place relating to the transfer.

4.4. If GEM Partnership processes a large quantity of information concerning the individual making the request, GEM Partnership might request that the individual specify the information or processing activities to which the request relates to specifically before the information is delivered. If such a request is required by GEM Partnership, then it shall be delivered promptly to the individual, taking into consideration the timeframes that subject access requests must be completed.

4.5. The individual's right to access their information shall not adversely affect the rights and freedoms of others and they will not be able to access the personal data of third parties without the explicit consent of that third party or if it is reasonable in all the circumstances to comply with the request without that third party's consent, taking into consideration any means to redact the personal data of any third party. Persons listed in the Appendix will decide whether it is appropriate to disclose the information to the individual on a case-by-case basis. This decision will involve balancing the individual's right of access of their personal data against the third party's rights in respect of their own personal data.

Note: an individual might not label their subject access request as such. Therefore, Company staff should always consider whether a request is a subject access request even when not called that. If in doubt, refer to the persons listed in the Appendix.

5. The Right to Rectification

5.1. An individual, or another data controller acting on an individual's behalf, has the right to obtain from GEM Partnership rectification of inaccurate or incomplete personal data concerning him or her. GEM Partnership must act on this request without undue delay.

5.2. Taking into account the purposes of the processing, the individual shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement stating what they would require to be completed.

5.3. GEM Partnership shall communicate any rectification of personal data to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. GEM Partnership shall inform the individual about those recipients if he or she requests it.

5.4. Where GEM Partnership, acting as a data processor, receives information from a data controller to rectify an individual's personal data, then GEM Partnership shall comply with this request unless this proves impossible or involves disproportionate effort.

5.5. In circumstances where GEM Partnership is unable to comply with the request as it proves impossible or involves disproportionate effort, GEM Partnership will document this in a privacy impact assessment or similar.

6. The Right to Erasure ('Right to be Forgotten')

6.1. An individual shall have the right to obtain from GEM Partnership, acting as data controller, the erasure of personal data concerning him or her without undue delay. GEM Partnership will be obliged to erase the individual's personal data without undue delay where one of the following grounds apply:

6.1.1. The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

6.1.2. An individual withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
6.1.3. An individual objects to the processing (based on either a public interest or a legitimate interest) and there are no overriding legitimate grounds for the processing, or an individual object to the processing for direct marketing purposes (including profiling related to direct marketing);
6.1.4. The personal data have been unlawfully processed;
6.1.5. The personal data have to be erased for compliance with a legal obligation; or
6.1.6. The personal data have been collected in relation to the offer of information society services to a child.
6.2. Where GEM Partnership, acting as data controller, has made the personal data public and is obliged to erase that personal data, GEM Partnership, taking into account available technology and the cost of implementation, shall take reasonable steps, including technological measures, to inform data controllers which are processing the personal data that an individual has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
6.3. GEM Partnership will not be obliged to erase information to the extent that processing is necessary:
6.3.1. For exercising the right of freedom of expression and information;
6.3.2. For compliance with a legal obligation which requires processing, or for the performance of a task carried out in the public interest or in the exercise of official authority vested in GEM Partnership acting as controller;
6.3.3. For reasons of public interest in the area of public health;
6.3.4. For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
6.3.5. For the establishment, exercise or defence of legal claims.
6.4. GEM Partnership shall communicate any erasure of personal data to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. GEM Partnership shall inform the individual about those recipients if an individual request it.
6.5. Where GEM Partnership, acting as a data processor, receives information from a data controller to erase an individual's personal data GEM Partnership shall comply with this request, unless this proves impossible or involves disproportionate effort.
6.6. In circumstances where GEM Partnership is unable to comply with the request as it proves impossible or involves disproportionate effort, GEM Partnership will document this in a privacy impact assessment or similar.

7. The Right to Restrict Processing

7.1. An individual will have the right to obtain from GEM Partnership, acting as a data controller, the restriction of processing his or her personal data where one of the following applies:
7.1.1. The accuracy of the personal data is contested by the individual, for a period enabling the Company to verify the accuracy of the personal data;
7.1.2. The processing is unlawful and the individual opposes the erasure of the personal data and requests the restriction of their use instead;

7.1.3. GEM Partnership no longer needs the personal data for the purposes of the processing, but they are required by an individual for the establishment, exercise or defence of legal claims;

7.1.4. The individual has objected to processing (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of GEM Partnership override those of the individual.

7.1.5. Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the individual's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

7.2. Where an individual who has successfully asked for their personal data to be restricted, then GEM Partnership will inform the individual before such a restriction is lifted.

7.3. GEM Partnership shall communicate any restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. GEM Partnership shall inform the individual about those recipients if he or she requests it.

7.4. Where GEM Partnership, acting as a data processor, receives information from a data controller to restrict processing an individual's personal data, GEM Partnership shall comply with this request, unless this proves impossible or involves disproportionate effort.

7.5. In circumstances where GEM Partnership is unable to comply with the request as it proves impossible or involves disproportionate effort, GEM Partnership will document this in a privacy impact assessment or similar.

8. The Right to Object to Processing

8.1. An individual, has the right to object to their personal data being processed or profiled based on a public interest or a legitimate interest.

8.2. Where GEM Partnership receives an objection to processing or profiling on the above, those listed in the Appendix will ensure that the processing and/or profiling ceases unless such persons can establish compelling grounds to continue to process the personal data. If this is the case the Data Controller will document this in a privacy impact assessment or similar.

9. Automated Decision-making Processes

9.1. An individual has the right not to be subjected to an automated decision-making process, including profiling, that produces a legal effect or a similarly significant effect on the individual.

9.2. However, it is possible to subject an individual to automated decision making processes, including profiling, where:

9.2.1. It is necessary for entering into or performance of a contract between the employer and the individual;

9.2.2. It is authorised by law; or

9.2.3. The individual has given their explicit consent.

9.3. GEM Partnership will ensure that suitable measures are in place to safeguard the individual's rights and freedoms and legitimate interests, under both Data Protection Laws and the Human Rights Act 1998, before this type of processing occurs for personal data.

9.4. GEM Partnership will only process sensitive (or special category) personal data where GEM Partnership has received either the explicit consent, there is a substantial public interest to do so, or in line with one of the other legal basis for processing conditions outlined in Annex 2. Again, GEM Partnership will ensure that suitable measures are in place to safeguard the individual's rights and freedoms and legitimate interests, under both Data Protection Laws and the Human Rights Act 1998, before this type of processing occurs for sensitive personal data. In addition, we will not retain this information any longer than is necessary, as outlined in our Data Retention Policy.

9.5. The safeguarding measures include:

9.5.1. Conducting a risk assessment as to what risks are posed to the individual's rights and freedoms;

9.5.2. Ensuring where the automated decision-making process is necessary for entering into or performance of a contract, that this is documented clearly by GEM Partnership;

9.5.3. Ensuring where explicit consent is given this is documented clearly by GEM Partnership.

9.6. Where there are other basis for processing special category data, this is clearly outlined in our privacy policies and consent documentation.

9.7. Company staff will be responsible for implementing the above safeguarding measures.

10. The Right to Withdraw Consent

10.1. Where GEM Partnership relies on an individual's consent to process their personal data then GEM Partnership will advise the individual that they have the right to withdraw his or her consent at any time.

10.2. Any Company staff who receives a request from an individual to withdraw their consent to processing their data will be responsible for issuing the individual with GEM Partnership's withdrawal of consent form. Once the form has been completed it should be given to the Data and Compliance Team to process the individual's request further.

11. Timing and Information to be Provided to the Individual

11.1. GEM Partnership shall provide information on action taken or not taken with regards to the individual data protection rights, inclusive, without undue delay and in any event within one month of receipt of the request. Where GEM Partnership does take action, then it may, where necessary, extend this period by a further two months, taking into account the complexity and number of the requests. GEM Partnership shall inform an individual of any extension within one month of receipt of the request, together with the reasons for the delay. Where GEM Partnership does not take action on the request of the individual then GEM Partnership will inform him or her on the possibility of lodging a complaint with the ICO and seeking a judicial remedy.

12. Charges

12.1. Where requests from an individual are manifestly unfounded or excessive, in particular because of their repetitive character, GEM Partnership may either:

12.1.1. Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

12.1.2. Refuse to act on the request.

12.2. GEM Partnership must demonstrate whether the request is manifestly unfounded or excessive.
12.3. Where the individual makes the request by electronic means GEM Partnership shall provide the information in a commonly used electronic form, unless otherwise requested by the individual.

13. Personal Data Breaches

13.1. GEM Partnership will need to act on any personal data protection breach it suspects or knows of when acting as either a data controller or a data processor.
13.2. Company staff must inform a member of the Data and Compliance Team where a personal data breach has either been reported to him or her or they themselves have identified a personal data breach.
13.3. Personal data breaches where GEM Partnership is the data controller, GEM Partnership will take measures to establish whether or not a personal data breach has occurred and follow the actions as required in the Data Breach Policy. This will include;
13.3.1. Conduct a risk assessment as to what level of risk the personal data breach poses/has occurred;
13.3.2. Conduct any relevant interviews or investigations of GEM Partnership's practices and/or Company staff to assess how the personal data breach occurred.
13.3.3. Implement measures and take steps to limit, contain and recover the breach
13.4. Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual, a member of the Data and Compliance Team responsible for alerting the ICO of any personal data breach without undue delay, but no later than 72 hours after having become aware of GEM Partnership's personal data breach. Where it is not possible to inform the ICO in this time those listed above will be responsible for explaining to the ICO the reasons for the delay.
13.5. If the personal data breach happens outside the UK then the Data and Compliance Team will be responsible for alerting the relevant supervisory authority in the effected jurisdiction.
13.6. If GEM Partnership are not able to provide the ICO/other relevant supervisory authority with all the relevant information related to the personal data breach then the company shall provide the information in phases without undue further delay.
13.7. A member of the Data and Compliance Team will be responsible for documenting any personal data breaches, including:
13.7.1. The facts relating to the personal data breach – including any investigations undertaken or statements taken from GEM Partnership's staff;
13.7.2. The effects of the personal data breach; and
13.7.3. The remedial action taken.
13.8. Personal data breaches where GEM Partnership is the data processor a member of the Data and Compliance Team will be responsible for alerting the relevant data controller as to the personal data breach that has been identified as soon as they are aware of the breach, having particular regard to any contractual obligations GEM Partnership has with the data controller.
13.9. Communicating personal data breaches to individuals, where a personal data breach has been identified, which results in a high risk to the rights and freedoms of individuals, the company will be responsible for informing those individuals effected by the personal data breach without undue delay.

13.10. For the avoidance of doubt there will be no need to inform individuals of a personal data breach where:

13.10.1. GEM Partnership has implemented appropriate technical and organisational protection measures

13.10.2. The nature of the Breach does not present a threat to an individuals data, due to encryption.

13.10.3. GEM Partnership has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.

13.10.4. It would involve disproportionate effort to tell all affected individuals. Instead, GEM Partnership will make a public communication or similar measure to tell all affected individuals.

14. Annex 1. Actions to take after a breach

Where there is a likely risk to individuals as a result of the breach

↓

Inform the ICO

↓

When a *data controller* notifies the ICO of a possible breach it must do the following:

1. **describe the nature of the *personal data breach* including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of *personal data* records concerned;**
2. **give the name and contact details of the data protection officer or other contact point where more information can be obtained;**
3. **describe the likely consequences of the *personal data breach*;**
4. **describe the measures taken or proposed to be taken by the controller to address the *personal data breach*, including where appropriate measures to mitigate its possible adverse effects.**

Where there is a high risk to individuals as a result of the breach

↓

Notify the individuals concerned as soon as is reasonably feasible

↓

When notifying individuals:

1. **describe the nature of the breach;**
2. **give the name and details of the data protection officer or other contact;**
3. **describe the likely consequences of the breach; and**
4. **describe the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.**

The main purpose behind notifying an individual of a breach is to outline the specific steps they should take to protect themselves. However, there are exceptions – communication with the data subject shall not be required if:

- **The *data controller* has implemented appropriate technical and organisational protection measures and those measures were applied to the data affected by the breach;**
- **The *data controller* has taken measures to ensure that the high risk to the rights and freedoms of data subjects is no longer likely to arise; or**
- **It would involve a disproportionate effort. In such a circumstances, there shall be a public communication whereby data subjects are informed in an equally effective manner.**

The information sent to individuals should be sent separate to any other communication and could be sent via multiple communication channels in order to ensure transparency. The information should also be presented in clear and plain language.

15. Annex 2. Legal Bases for processing personal data

15.1. The lawfulness of processing conditions for personal data are:

15.1.1. Consent of the individual for one or more specific purposes.

15.1.2. Processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract.

15.1.3. Processing is necessary for compliance with a legal obligation to which the controller is subject to.

15.1.4. Processing is necessary to protect the vital interests of the individual or another person.

15.1.5. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

15.1.6. Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of personal data, in particular where the individual is a child.

16. The lawfulness of processing conditions for sensitive personal data are:

16.1. Explicit consent of the individual for one or more specified purposes, unless reliance on consent is prohibited by EU or Member State law.

16.2. Processing is necessary for carrying out data controller's obligations under employment, social security or social protection law, or a collective agreement, providing for appropriate safeguards for the fundamental rights and interests of the individual.

16.3. Processing is necessary to protect the vital interests of the individual or another individual where the individual is physically or legally incapable of giving consent.

16.4. In the course of its legitimate activities, processing is carried out with appropriate safeguards by a foundation, association or any other not-for-profit body, with a political, philosophical, religious or trade union aim and on condition that the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without the consent of the individual.

16.5. Processing relates to personal data which are manifestly made public by the individual.

16.6. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

16.7. Processing is necessary for reasons of substantial public interest on the basis of EU or Member State law which shall be proportionate to the aim pursued, respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.

16.8. Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or

Member State law or a contract with a health professional and subject to the necessary conditions and safeguards.

16.9. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy.

16.10. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard fundamental rights and interests of the individual.

17. Confidentiality and Information Sharing

17.1. In an allegations management meeting or during the initial assessment of a reported welfare case, the agencies involved should share all relevant information they have about the individual who is the subject of the allegation and about the alleged victim.