Company Name:	Highgrade Recruitment Ltd
Document	Data Protection: Policy Procedure
Date	March 2020
Version	1

CONTENT

Highgrade Recruitment Ltd are committed to protecting their employees personal data.
All organisations that process *personal data* are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU 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.

As a recruitment business Highgrade Recruitment Ltd 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 and the policy by law.

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

In this policy the following terms have the following meanings:

'*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;

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

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

'*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.

'*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*;

'*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.

'*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;

'*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;

'*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.

* For the purposes of this policy we use the term '*personal data*' to include '*sensitive personal data*' except where we specifically need to refer to *sensitive personal data*.

'*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).

All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.

The Company processes *personal data* in relation to its own staff, work-seekers and individual client contacts and is a *data controller* for the purposes of the Data Protection Laws. The Company has registered with the ICO and its registration number is ZA167542.

Highgrade Recruitment Ltd may hold *personal data* on individuals for the following purposes:

- Staff administration;
- Advertising, marketing and public relation
- Accounts and records;
- 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
- Administration and *processing* of clients' *personal data* for the purposes of supplying/introducing work-seekers

The data protection principles

The Data Protection Laws require Highgrade Recruitment Ltd, 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:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- Kept for no longer than is necessary for the purposes for which the *personal data* are processed;
- 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
- The *data controller* shall be responsible for, and be able to demonstrate, compliance with the principles.

Legal bases for processing

Highgrade Recruitment Ltd will only process *personal data* where it has a legal basis for doing so (see Annex A). Where the Company does not have a legal reason for *processing personal data* any processing will be a breach of the Data Protection Laws.

Highgrade Recruitment Ltd 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 and those people listed in the Appendix shall be responsible for doing this.

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)), the Company will establish that it has a legal reason for making the transfer.

Privacy by design and by default

Highgrade Recruitment Ltd 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:

- data minimisation (i.e. not keeping data for longer than is necessary)
- *pseudonymisation* (i.e. references to replace data)
- anonymization (i.e. encryptions for privacy protection)
- cyber security (i.e. the protection of computer systems)

Highgrade Recruitment Ltd 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. The Company may provide this information orally if requested to do so by the individual.

Privacy notices

Where Highgrade Recruitment Ltd collects *personal data* from the individual, the Company will give the individual a privacy notice at the time when it first obtains the *personal data*.

Where the Company 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 the Company 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).

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

Subject access requests

The individual is entitled to access their *personal data* on request from the *data controller*.

Rectification

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

If the Company 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 the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

Erasure

The individual or another *data controller* at the individual's request, has the right to ask the Company to erase an individual's *personal data.*

If the Company 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). The Company cannot keep a record of individuals whose data it has erased so the individual may be contacted

again by the Company should the Company come into possession of the individual's *personal data* at a later date.

If the Company 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.

If the Company 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 the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

Restriction of *processing*

The individual or a *data controller* at the individual's request, has the right to ask the Company to restrict its *processing* of an individual's *personal data* where:

- The individual challenges the accuracy of the *personal data*;
- The *processing* is unlawful and the individual opposes its erasure;
- The Company 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
- The individual has objected to *processing* (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the individual.

If the Company 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 the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

Data portability

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

- The *processing* is based on the individual's *consent* or a contract; and
- The *processing* is carried out by automated means.

Where feasible, the Company will send the *personal data* to a named third party on the individual's request.

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.

The Company 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.

The individual has the right to object to their *personal data* for direct marketing.

Enforcement of rights

All requests regarding individual rights should be sent to the person whose details are listed in the Appendix.

Highgrade Recruitment Ltd 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 one month of receipt of the request. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

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

Automated decision making

The Company 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:

- Is necessary for the entering into or performance of a contract between the *data controller* and the individual;
- Is authorised by law; or
- The individual has given their explicit *consent*.

Highgrade Recruitment Ltd will not carry out any automated decision-making or *profiling* using the *personal data* of a child.

Reporting *personal data* breaches

All data breaches should be referred to the persons whose details are listed in the Appendix. (i.e. Claire James).

Personal data breaches where the Company is the *data controller*:

Where the Company establishes that a *personal data breach* has taken place, the Company 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 the Company will notify the ICO.

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

Personal data breaches where the Company is the *data processor*:

The Company will alert the relevant *data controller* as to the *personal data breach* as soon as they are aware of the breach.

Communicating *personal data breaches* to individuals

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

Highgrade Recruitment Ltd will not be required to tell individuals about the *personal data breach* where:

- The Company 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.
  The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to tell all affected individuals. Instead, the Company shall make a public communication or similar measure to tell all affected individuals.

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:

- Right to respect for private and family life (Article 8).
- Freedom of thought, belief and religion (Article 9).
- Freedom of expression (Article 10).
- Freedom of assembly and association (Article 11).
- Protection from discrimination in respect of rights and freedoms under the HRA (Article 14).

If you have a complaint or suggestion about the Company's handling of *personal data* then please contact the person whose details are listed in the Appendix to this policy, (i.e. Claire James).

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

At Highgrade Recruitment Ltd the following names are persons responsible for:

- adding, amending or deleting *personal data*;
- responding to subject access requests/requests for rectification, erasure, restriction data portability, objection and automated decision making processes and profiling;
- reporting data breaches/dealing with complaints; and/or
- details of the Data Protection Officer where applicable

Cheryl Kellard – Administration Worker

Claire James - Manager

- **The lawfulness of *processing* conditions for *personal data* are:**

  - *Consent* of the individual for one or more specific purposes.
  - *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.
  - *Processing* is necessary for compliance with a legal obligation that the controller is subject to.
  - *Processing* is necessary to protect the vital interests of the individual or another person.
  - *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*.
  - *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.

- **The lawfulness of *processing* conditions for *sensitive personal data* are:**

- Explicit *consent* of the individual for one or more specified purposes, unless reliance on *consent* is prohibited by EU or Member State law.
- *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.
- *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*.
- 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.
- *Processing* relates to *personal data* which are manifestly made public by the individual.
- *Processing* is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- *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.
- *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.
- *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.
- *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.

Data Protection Procedures

Only those listed in the Appendix are permitted to add, amend or delete personal data from the Company's database(s) ('database' includes paper records or records stored electronically).

All Company staff are responsible for notifying those listed in the Appendix 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 in the Appendix where any request for data portability, objection to *processing* or where *consent* to process has been withdrawn and has been received from the individual.

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 the Company for damages from an employee, work-seeker or client contact.

A failure to observe the contents of this procedure policy will be treated as a disciplinary offence.

In addition all Highgrade Recruitment Ltd Staff should ensure that adequate security measures are in place to limit the risk of *personal data breaches*. For example:

- Staff should lock their computer screens when they are not in use.
- All devices, whether company or personal devices (including but not limited to computers, mobile phones, other hand-held devices) containing personal data relating to the services of the Company shall be encrypted and password protected.
- Staff should not disclose their passwords to anyone.
- 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 those listed in the Appendix of the error so that any risk of a *personal data breach* can be limited.
- Personnel files (whether for internal staff or work-seekers) and other personal data should be stored securely to prevent unauthorised access. They should not be removed from their usual place of storage without good reason.
- Personnel files (whether for internal staff or work-seekers) should always be locked away when not in use and when in use should not be left unattended.
- Personal data should only be stored for the periods set out in the Company's data retention policy.
- *Processing* includes the destruction or disposal of personal data. Therefore staff should take care to destroy or dispose of personal data safely and securely. Such material should be shredded or stored as confidential waste awaiting safe destruction.

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

1. The right to be informed of what information the Company holds on them – this is typically given to the individual in a privacy notice;
2. The right of access to any personal data that the Company holds on them – this is usually referred to as a 'subject access request';
3. The right to rectification of personal data that the individual believes is either inaccurate or incomplete;
4. The right to erasure of their personal data in certain circumstances;
5. The right to restrict *processing* of their personal data;
6. The right to data portability of their personal data in specific circumstances;
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;
8. The right not to be subjected to automated decision making and *profiling*; and
9. The right to withdraw *consent* where it was relied upon to process their personal data.

1. The right to be informed

Any individual whose *personal data* is processed by the staff at Highgrade Recruitment Ltd 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 the Company's website privacy notice or be given a copy of a privacy notice. This privacy notice should be issued in instances where either:

a) the Company collects/processes data directly from the individual; or
b) the Company has not collected/processed the data from the individual directly.

The privacy notice should include the information set out in Table 1 (below).

In addition:

a) Where personal data has been collected **from the individual** the privacy notice/GDPR will need to be issued at the point the data is collected. At Highgrade Recruitment Ltd when new clients are signed up the GDPR/Privacy Notice form is issued and signed. Where the Company intends to further process the personal data for a purpose other than that for which the personal data was collected, the Company shall provide the individual, prior to that further *processing*, with information on that other purpose and with any relevant further information in updated privacy notice.

b) Where personal data has **not been obtained from the individual**, the Company 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.

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

Table 1: Privacy information to be given to the individual

	Where the Company collects data from the individual:	Where personal data has not been obtained from the individual:
• The identity and contact details of the Company 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 countries and the safeguards in place. (Not currently applicable to Highgrade Recruitment Ltd)	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
• 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

2. The right to access ('subject access request')

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

An individual will be entitled to the following information:

- Confirmation that their personal data is or is not being processed;
- Access to the personal data undergoing *processing*;
- The purposes of the *processing*;
- The categories of personal data concerned;
- 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;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request from the Company rectification or erasure of personal data or restriction of *processing* of personal data concerning the individual or to object to such *processing*;
- The right to lodge a complaint with the ICO or any other relevant *supervisory authority*;
- Where the personal data are not collected from an individual, any available information as to the source of that information;
- 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.

If the Company 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.

If the Company processes a large quantity of information concerning the individual making the request, the Company 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 the Company then it shall be delivered promptly to the individual, taking into consideration the timeframes that subject access requests must be completed.

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.

> **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.

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.

3. The right to rectification

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

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.

The Company 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. The Company shall inform the individual about those recipients if he or she requests it.

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

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

4. The right to erasure ('right to be forgotten')

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

- The *personal data* are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- An individual withdraws *consent* on which the *processing* is based, and where there is no other legal ground for the *processing*;
- 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 objects to the *processing* for direct marketing purposes (including *profiling* related to direct marketing);
- The *personal data* have been unlawfully processed;
- The *personal data* have to be erased for compliance with a legal obligation; or
- The *personal data* have been collected in relation to the offer of information society services to a child.

Where the Company, acting as *data controller*, has made the *personal data* public and is obliged to erase that *personal data*, the Company, 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*.

The Company will not be obliged to erase information to the extent that *processing* is necessary:

- For exercising the right of freedom of expression and information;

- 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 the Company acting as controller;
- For reasons of public interest in the area of public health;
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
- For the establishment, exercise or defence of legal claims.

The Company 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. The Company shall inform the individual about those recipients if an individual requests it.

Where the Company, acting as a *data processor*, receives information from a *data controller* to erase an individual's *personal data* the Company shall comply with this request, unless this proves impossible or involves disproportionate effort.

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

5. The right to restrict *processing*

An individual will have the right to obtain from the Company, acting as a *data controller*, the restriction of processing his or her personal data where one of the following applies:

- 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*;
- The *processing* is unlawful and the individual opposes the erasure of the *personal data* and requests the restriction of their use instead;
- The Company 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;
- The individual has objected to *processing* (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the individual.

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.

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

The Company 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. The Company shall inform the individual about those recipients if he or she requests it.

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

6. The right to access ('subject access request')

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

An individual will be entitled to the following information:

- Confirmation that their personal data is or is not being processed;
- Access to the personal data undergoing *processing*;
- The purposes of the *processing*;
- The categories of personal data concerned;
- 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;
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- The existence of the right to request from the Company rectification or erasure of personal data or restriction of *processing* of personal data concerning the individual or to object to such *processing*;
- The right to lodge a complaint with the ICO or any other relevant *supervisory authority*;
- Where the personal data are not collected from an individual, any available information as to the source of that information;
- 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.

If the Company 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.

If the Company processes a large quantity of information concerning the individual making the request, the Company 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 the Company then it shall be delivered promptly to the individual, taking into consideration the timeframes that subject access requests must be completed.

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

> **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.

own personal data.

7. The right to rectification

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

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.

The Company 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. The Company shall inform the individual about those recipients if he or she requests it.

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

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

8. The right to erasure ('right to be forgotten')

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

- The *personal data* are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- An individual withdraws *consent* on which the *processing* is based, and where there is no other legal ground for the *processing*;
- 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 objects to the *processing* for direct marketing purposes (including *profiling* related to direct marketing);
- The *personal data* have been unlawfully processed;
- The *personal data* have to be erased for compliance with a legal obligation; or
- The *personal data* have been collected in relation to the offer of information society services to a child.

Where the Company, acting as *data controller*, has made the *personal data* public and is obliged to erase that *personal data*, the Company, 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*.

The Company will not be obliged to erase information to the extent that *processing* is necessary:

- For exercising the right of freedom of expression and information;
- 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 the Company acting as controller;
- For reasons of public interest in the area of public health;
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or
- For the establishment, exercise or defence of legal claims.

The Company 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. The Company shall inform the individual about those recipients if an individual requests it.

Where the Company, acting as a *data processor*, receives information from a *data controller* to erase an individual's *personal data* the Company shall comply with this request, unless this proves impossible or involves disproportionate effort.

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

9. The right to restrict *processing*

An individual will have the right to obtain from the Company, acting as a *data controller*, the restriction of processing his or her personal data where one of the following applies:

- 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*;
- The *processing* is unlawful and the individual opposes the erasure of the *personal data* and requests the restriction of their use instead;
- The Company 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;
- The individual has objected to *processing* (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the individual.

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.

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

The Company 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. The Company shall inform the individual about those recipients if he or she requests it.

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

The Company 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*.

Company staff must inform those persons listed in the Appendix where a *personal data* breach has either been reported to him or her or they themselves have identified a *personal data breach*.

1. *Personal data* breaches where the Company is the *data controller*:

Those listed in the Appendix will take measures to establish whether or not a *personal data breach* has occurred. Those persons will:

- [Conduct a risk assessment as to what level of risk the *personal data breach* poses/has occurred]
- [Conduct any relevant interviews or investigations of the Company's practices and/or Company staff to assess how the *personal data breach* occurred]
- [Implement measures and take steps to limit, contain and recover the breach]
- [Inform all persons affected by the breach]

Unless the *personal data breach* is unlikely to result in a risk to the rights and freedoms of an individual, then those listed in the Appendix will be responsible for alerting the ICO of any *personal data breach* without undue delay, but no later than 72 hours after having become aware of the Company's *personal data breach*. Where it is not possible to inform the ICO in this time those listed in the Appendix will be responsible for explaining to the ICO the reasons for the delay.

If the *personal data breach* happens outside the UK then those listed in the Appendix will be responsible for alerting the relevant *supervisory authority* in the effected jurisdiction.

If those listed in the Appendix are not able to provide the ICO/other relevant *supervisory authority* with all the relevant information related to the *personal data breach* then those persons shall provide the information in phases without undue further delay.

Those listed in the Appendix will be responsible for documenting any *personal data breaches*, including:

- The facts relating to the *personal data breach* – including any investigations undertaken or statements taken from the Company's staff;
- The effects of the *personal data breach*; and
- The remedial action taken.

2. *Personal data breaches* where the Company is the *data processor*:

Those listed in the Appendix 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 the Company has with the *data controller*.

3. 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, those listed in the Appendix will be responsible for informing those individuals effected by the *personal data breach* without undue delay.

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

- The Company has implemented appropriate technical and organisational protection measures to use 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.
- The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
- It would involve disproportionate effort to tell all affected individuals. Instead, those listed in the Appendix shall, on behalf of the Company, make a public communication or similar measure to tell all affected individuals.

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.

A more detailed flowchart is available in the Article 29 Working party's Guidance on personal data breaches. See the REC's table of resources.

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.

Those listed in the Appendix will keep written records of the *processing* activities of the Company. The records must be in writing (which can be in electronic form) and must include the following information:

- The name and contact details of the *data controller* or *data controller*'s representative and any joint controllers;
- The purposes of the *processing*;
- A description of the categories of the data subjects and of the categories of the *personal data*;
- The categories of recipients to whom *personal data* have or will be disclosed to, including to those internationally;
- Any transfers of *personal data* internationally, including the identification of the third country or international organisation to which the data is transferred;
- The envisaged time limits placed on an individual's right to erasure; and
- Where possible, a description of the technical and security measures that have been utilised to alleviate data-related risks.

The Company will also document:

- Information required for privacy notices;
- Records of *consent*;
- Controller-processor contracts;
- The location of *personal data*;
- Data Protection Impact Assessment reports;
- Records of *personal data breaches*;
- Information required for *processing sensitive personal data* or criminal convictions/offences data.

The Company will make these records available to the ICO upon request.