EU GDPR & UK DPA 2018 Policy

V1.1 22/02/24

This policy sets out how P2G Associates (P2G) implements the Data Protection Laws. It should be read in conjunction with the Data Protection Procedure and current active guidance from the ICO.

As a consequence of Brexit the Uk having left the EU, the UK implemented it's version of the EU GDPR entitled DPA 2018. There are some notable differences between the two legislations and P2G acknowledges both and prioritises UK DPA 2018 whilst maintaining compliance with EU GDPR.

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).

P2G processes personal data in relation to its own staff, candidates and individual client contacts and is a data controller for the purposes of the Data Protection Laws. P2G has registered with the ICO and its registration number is ZB667789 – details available *here*.

P2G may hold personal data on individuals for the following purposes:

- Staff administration;
- Advertising, marketing and public relations;
- Accounts and records;
- Administration and processing of candidates' 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 candidates to suppliers or client's;
- Contractual information for both public and private customers

1. The data protection principles

The Data Protection Laws require P2G 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:

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

2. Legal bases for processing

P2G will only process personal data where it has a legal basis for doing so (see Annex A). Where P2G does not have a legal reason for processing personal data any processing will be a breach of the Data Protection Laws.

P2G 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.

P2G only works in a contracts that are deemed as business to business agreement (B2B) we currently have no Business to Consumer (B2C) engagement.

Before transferring personal data to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as, third party employers, umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back-office support), P2G will establish that it has a legal reason for making the transfer.

3. Privacy by design and by default

P2G 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;
- anonymization; and
- cyber security. We hold a valid cyber essentials certificate

P2G 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. P2G may provide this information orally if requested to do so by the individual.

4. Privacy notices

Where P2G collects personal data from the individual, P2G will give the individual a privacy notice at the time when it first obtains the personal data.

Where P2G 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 P2G 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 P2G intends to further process the personal data for a purpose other than that for which the data was initially collected, P2G will give the individual information on that other purpose and any relevant further information before it does the further processing.

5. Subject access requests

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

6. Rectification

The individual or another data controller at the individual's request, has the right to ask P2G to rectify any inaccurate or incomplete personal data concerning an individual.

If XXXXXXXXX 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 P2G will not be in a position to audit those third parties to ensure that the rectification has occurred.

7. Erasure

The individual or another data controller at the individual's request, has the right to ask P2G to erase an individual's personal data.

If P2G 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). P2G cannot keep a record of individuals whose data it has erased so the individual may be contacted again by P2G should P2G come into possession of the individual's personal data at a later date.

If P2G 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 P2G 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 P2G will not be in a position to audit those third parties to ensure that the rectification has occurred.

8. Restriction of processing

The individual or a data controller at the individual's request, has the right to ask P2G 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;
- P2G 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 P2G override those of the individual.

If P2G 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 P2G will not be in a position to audit those third parties to ensure that the rectification has occurred.

9. Data portability

The individual shall have the right to receive personal data concerning him or her, which he or she has provided to P2G, 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, P2G will send the personal data to a named third party on the individual's request.

10. 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.

P2G 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.

11. Enforcement of rights

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

P2G 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. P2G may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where P2G considers that a request under this section is manifestly unfounded or excessive due to the request's repetitive nature P2G may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

12. Automated decision making

P2G 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.

P2G will not carry out any automated decision-making or profiling using the personal data of a child.

13. Direct marketing

P2G is subject to certain rules when marketing our clients and candidates. Individuals prior consent is required for electronic direct marketing. There is a limited exception for existing clients and candidates which allows us to send marketing texts and e-mails if we have obtained their contact details in the course of working finding services to that individual, P2G are marketing similar products or services to individuals and P2G gave that individual an opportunity to opt out of marketing when first collecting their details and in every subsequent message. We ensure that any 3rd party data purchased or platforms used in the business, meet the standards for GDPR and we review their policy.

If an individual objects to direct marketing, it is essential that this is actioned in a timely manner and their details will be suppressed as soon as possible. P2G can retain just enough information to ensure that marketing preferences are respected in the future.

14. Provision of candidate information following an audit request

In the event of a client audit request the following documents have been identified as requiring certain specific confidential information to be redacted. Following completion of the audit, confirmation is to be provided that all documents detailed in this policy have been destroyed. Workforce will be able to provide documents related only to the client the audit was facilitated for due to data protection and commercial agreements.

Document	Information to be redacted
ID or Right to Work	Passport number Passport ID National ID card number National ID card reference Candidate address on National ID card
Payslip	Candidate address Employer name NI number
Candidate Registration Form	Candidate address Candidate telephone number Candidate email Candidate D.O.B Reference name, telephone number and email

Document	Information to be redacted
Contract of Employment	Employer's name and address Candidates address

Any other documents requested during an audit must be reviewed by People and Compliance Manager before being supplied.

15. Reporting personal data breaches

All data breaches should be referred to the persons whose details are listed in the Appendix.

a. Personal data breaches where P2G **is the data controller:**

Where P2G establishes that a personal data breach has taken place, P2G 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 P2G will notify the ICO.

Where the personal data breach happens outside the UK, P2G shall alert the relevant supervisory authority for data breaches in the effected jurisdiction.

b. Personal data breaches where P2G **is the data processor:**

P2G will alert the relevant data controller as to the personal data breach as soon as they are aware of the breach.

c. Communicating personal data breaches to individuals

Where P2G has identified a personal data breach resulting in a high risk to the rights and freedoms of any individual, P2G shall tell all affected individuals without undue delay.

P2G will not be required to tell individuals about the personal data breach where:

P2G 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.

P2G 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, P2G 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 P2G handling of personal data then please contact the person whose details are listed in the Appendix to this policy.

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

Declan Ross-Thomasis P2G's Data Protection Officer and is responsible for: -

- adding, amending or deleting personal data;
- responding to subject access requests/requests for rectification, erasure, restriction data portability, objection, automated decision-making processes and profiling and withdrawal of consent;
- reporting data breaches/dealing with complaints; and/or
- Carrying out any appropriate internal disciplinary action if necessary.

a) The lawfulness of processing conditions for personal data are:

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

b) The lawfulness of processing conditions for sensitive personal data are:

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

End of Policy