Data Protection Policy

www.paritasrecruitment.com

Last updated: June 2019

Table of Contents

Introduction

Paritas Recruitment takes its responsibilities with regard to the management of the requirements of the General Data Protection Regulation (GDPR) very seriously. *Paritas Recruitment* obtains, uses, stores and otherwise processes personal data relating to potential staff, potential clients, clients, suppliers, business contacts, staff, former staff and clients, website users and contacts and other people the organisation has a relationship with or may need to contact, collectively referred to in this policy as data subjects. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

When processing personal data, the company is obliged to fulfil individuals' reasonable expectations of privacy by complying with GDPR and other relevant data protection legislation (data protection law).

This policy therefore seeks to ensure that we:

1. Are clear about how personal data must be processed and the company's expectations for all those who process personal data on its behalf;
2. Comply with the data protection law and with good practice;
3. Protect the company's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
4. Protect the company from risks of personal data breaches and other breaches of data protection law.

Scope

This policy applies to all personal data we process regardless of the location where that personal data is stored (e.g. on an employee's own device) and regardless of the data subject. All staff and others processing personal data on the company's behalf must read it. A failure to comply with this policy will result in disciplinary action.

The Directors are responsible for ensuring that all company staff within their area of responsibility comply with this policy and should implement appropriate practices, processes, controls and training to ensure that compliance.

The company's Data Protection Officer (DPO) and Information Compliance Officer is Mr Leigh Albrecht, he can be reached at contacus@paritasrecruitment.com.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ….plus any other information relating to individuals

Definitions

Automated Decision-Making (ADM): when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not automated processing.

Profiling: 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 individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

Data Controller: the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in accordance with the GDPR. The company is the Data Controller of all personal data relating to it and used delivering education and training, conducting research and all other purposes connected with it including business purposes.

Data Subject: a living, identified or identifiable individual about whom we hold personal data.

Data Protection impact assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person appointed as such under the GDPR and in accordance with its requirements. A DPO is responsible for advising the company (including its employees) on their obligations under Data Protection Law, for monitoring compliance with data protection law, as well as with the company's polices, providing advice, cooperating with the ICO and acting as a point of contact with the ICO.

Information Commission's Office (ICO): the ICO is the UK's independent body set up to uphold information rights. Information on how to contact ICO and make a complaint can be found online at: https://ico.org.uk/.

Personal Data: any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes sensitive personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the data subject. It can be an act or omission.

Privacy by Design and Default: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to data subjects when the company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, staff and client privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering processing related to a specific purpose.

Processing or Process: any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to personal data from its creation to its destruction, including both creation and destruction.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Data Protection Law

The Data Protection Act 1998 describes how organisations – including *Paritas Recruitment* – must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly, lawfully and in a transparent manner.
2. Be obtained only for specific lawful purposes.
3. Be adequate, relevant and not excessive.
4. Be accurate and kept up to date.
5. Not be held for any longer than necessary.
6. Processed in accordance with the rights of data subjects.
7. Be protected in appropriate ways.
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

Data Subjects' Rights

Data subjects have rights in relation to the way we handle their personal data. These include the following rights:

1. Where the legal basis of our processing is Consent, to withdraw that Consent at any time;
2. To ask for access to the personal data that we hold (see below);
3. To prevent our use of the personal data for direct marketing purposes
4. To object to our processing of personal data in limited circumstances

5. To ask us to erase personal data without delay:
    a. If it is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
    b. If the only legal basis of processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can process that personal data;
    c. If the data subject objects to our processing where the legal basis is the pursuit of a legitimate interest or the public interest and we can show no overriding legitimate grounds or interest;
    d. If the data subject has objected to our processing for direct marketing purposes;
    e. If the processing is unlawful.
6. To ask us to rectify inaccurate data or to complete incomplete data;
7. To restrict processing in specific circumstances e.g. where there is a complaint about accuracy;
8. To ask us for a copy of the safeguards under which personal data is transferred outside of the EU;
9. The right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with the company; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards;
10. To prevent processing that is likely to cause damage or distress to the data subject or anyone else;
11. To be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
12. To make a complaint to the ICO; and
13. In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

We will verify the identity of an individual requesting data under any of the rights listed

Requests (including for data subject access – see below) will be complied with, usually within one month of receipt. We will immediately forward any Data Subject Access Request we receive to the Information Compliance Officer. A charge can be made for dealing with requests relating to these rights only if the request is excessive or burdensome.

Accountability

The company must implement appropriate technical and organisational measures in an effective manner to ensure compliance with data protection principles. The company is responsible for, and must be able to demonstrate compliance with, the data protection principles.

We must therefore apply adequate resources and controls to ensure and to document GDPR compliance including:

1. Appointing a suitably qualified DPO;
2. Implementing Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) where processing presents a high risk to the privacy of data subjects;
3. Integrating data protection into our policies and procedures, in the way personal data is handled by us and by producing required documentation such as Privacy Notices, Records of Processing and records of Personal Data Breaches;

4. Training staff on compliance with Data Protection Law; and
5. Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

Responsibilities

Company Responsibilities

As the Data Controller, the company is responsible for establishing policies and procedures in order to comply with data protection law.

Data Protection Officer Responsibilities

The DPO is responsible for:

(a) Advising the company and its staff of its obligations under GDPR
(b) Monitoring compliance with this Regulation and other relevant data protection law, the company's policies with respect to this and monitoring training and audit activities relate to GDPR compliance
(c) To provide advice where requested on data protection impact assessments
(d) To cooperate with and act as the contact point for the Information Commissioner's Office
(e) The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Staff Responsibilities

Staff members who process personal data about clients, staff, candidates, suppliers or any other individual must comply with the requirements of this policy. Staff members must ensure that:

(a) All personal data is kept securely;
(b) No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party;
(c) Personal data is kept in accordance with the company's retention schedule;
(d) Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Information Compliance Officer;
(e) Any data protection breaches are swiftly brought to the attention of the Information Compliance Officer and the Data Protection Officer and that they support the Information Compliance Officer in resolving breaches;
(f) Where there is uncertainty around a data protection matter advice is sought from the Information Compliance Officer and the Data Protection Officer.

Where members of staff are responsible for supervising service providers doing work which involves the processing of personal information, they must ensure that those service providers are aware of the Data Protection principles.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from the Information Compliance Officer or the Data Protection Officer.

Third-Party Data Processors

Where external companies are used to process personal data on behalf of the company, responsibility for the security and appropriate use of that data remains with the company.

Where a third-party data processor is used:

(a) A data processor must be chosen which provides sufficient guarantees about its security measures to protect the processing of personal data;
(b) Reasonable steps must be taken that such security measures are in place;
(c) A written contract establishing what personal data will be processed and for what purpose must be set out;
(d) A data processing agreement, available from the Information Compliance Officer, must be signed by both parties.

For further guidance about the use of third-party data processors please contact the Information Compliance Officer.

Contractors, Short-Term and Voluntary Staff

The company is responsible for the use made of personal data by anyone working on its behalf. Managers who employ contractors, short term or voluntary staff must ensure that they are appropriately vetted for the data they will be processing. In addition, managers should ensure that:

(a) Any personal data collected or processed in the course of work undertaken for the company is kept securely and confidentially;
(b) All personal data is returned to the company on completion of the work, including any copies that may have been made. Alternatively, that the data is securely destroyed and the company receives notification in this regard from the contractor or short term / voluntary member of staff;
(c) The company receives prior notification of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor;
(d) Any personal data made available by the company, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from the company;
(e) All practical and reasonable steps are taken to ensure that contractors, short term or voluntary staff do not have access to any personal data beyond what is essential for the work to be carried out properly.

For further guidance about the access of contractors, short-term and voluntary staff please contact the Information Compliance Officer.

Client Responsibilities

Clients are responsible for:

(a) Familiarising themselves with the Privacy Notice provided when they register with the company;
(b) Ensuring that their personal data provided to the company is accurate and up to date.

Data Storage / Privacy

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or the Data Protection Officer. When data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts.

- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by approved security software and a firewall.

Data Use

Personal data is of no value to *Paritas Recruitment* unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft.

- When working with personal data, employees should ensure the screens of their computers are always locked when unattended.
- Personal Data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of data.

Data Subject Access Requests

Data subjects have the right to receive copy of their personal data which is held by the company. In addition, an individual is entitled to receive further information about the company's processing of their personal data as follows:

1. The purposes
2. The categories of personal data being processed
3. Recipients/categories of recipient
4. Retention periods
5. Information about their rights
6. The right to complain to the ICO,
7. Details of the relevant safeguards where personal data is transferred outside the EEA
8. Any third-party source of the personal data

You should not allow third parties to persuade you into disclosing personal data without proper authorisation. For example, candidates' parents do not have an automatic right to gain access to their child's data.

The entitlement is not to documents per se (which may however be accessible by means of the Freedom of Information Act, subject to any exemptions and the public interest), but to such personal data as is contained in the document. The right relates to personal data held electronically and to limited manual records.

You should not alter, conceal, block or destroy personal data once a request for access has been made. You should contact the Information Compliance team before any changes are made to personal data which is the subject of an access request.

Reporting a Personal Data Breach

The GDPR requires that we report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the Personal data breach results in a high risk to the data subject, he/she also has to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made, or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or the ICO where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, you should immediately contact the Information Compliance Officer at contacus@paritasrecruitment.com and follow the instructions in the personal data breach procedure. You must retain all evidence relating to personal data breaches in particular to enable the company to maintain a record of such breaches, as required by the GDPR.

Limitations on the Transfer of Personal Data

The GDPR restricts data transfers to countries outside the EU in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer personal data originating in one country across borders when you transmit or send that data to a different country or view/access it in a different country.

You may only transfer personal data outside the EU if one of the following conditions applies:

1. The European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subjects' rights and freedoms. The countries currently approved can be found here: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.
2. Appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
3. The data subject has provided explicit Consent to the proposed transfer after being informed of any potential risks; or
4. The transfer is necessary for one of the other reasons set out in the GDPR including:
5. The performance of a contract between us and the data subject (e.g. students' mandatory year abroad in an overseas institution/placement),
6. Reasons of public interest,
7. To establish, exercise or defend legal claims or
8. To protect the vital interests of the data subject where the data subject is physically or legally incapable of giving Consent.

The company at present doesn't transfer any data personal or otherwise out of the EU.

Record Keeping

The GDPR requires us to keep full and accurate records of all our data processing activities. You must keep and maintain accurate corporate records reflecting our processing, including records of data subjects' Consents and procedures for obtaining Consents, where Consent is the legal basis of processing.

These records should include, at a minimum, the name and contact details of the company as Data Controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place.

Records of personal data breaches must also be kept, setting out:

1. The facts surrounding the breach
2. Its effects; and
3. The remedial action taken

Training and Audit

We are required to ensure that all company staff undergo adequate training to enable them to comply with data protection law. We must also regularly test our systems and processes to assess compliance.

We regularly review all the systems and processes under our control to ensure they comply with this policy.

Data Privacy by Design and Default And Data Protection Impact Assessments (DPIAS)

We are required to implement privacy-by-design measures when processing personal data, by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data-protection principles. The company must ensure therefore that by default only personal data which is necessary for each specific purpose is processed. The obligation applies to the volume of personal data collected, the extent of the processing, the period of storage and the accessibility of the personal data. In particular, by default, personal data should not be available to an indefinite number of persons.

The company must also conduct DPIAs in respect of high-risk processing before that processing is undertaken.

You should conduct a DPIA (and discuss your findings with the DPO) in the following circumstances:

1. The use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
2. Automated processing including profiling;
3. Large scale processing of sensitive (special category) data; and
4. Large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

1. A description of the processing, its purposes and the Data Controller's legitimate interests if appropriate;
2. An assessment of the necessity and proportionality of the processing in relation to its purpose;
3. An assessment of the risk to individuals; and
4. The risk-mitigation measures in place and demonstration of compliance.

Direct Marketing

We are subject to certain rules and privacy laws when marketing to our candidates, clients and any other potential user of our services.

For example, a data subject's prior Consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers (e.g. current candidates) known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

A data subject's objection to direct marketing must be promptly honoured. If a data subject opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Sharing Personal Data

In the absence of Consent, a legal obligation or other legal basis of processing, personal data should not generally be disclosed to third parties unrelated to the company (e.g. candidates' parents, members of the public, private property owners).

Some bodies have a statutory power to obtain information (e.g. regulatory bodies such as the Health & Care Professions Council, the Nursing and Midwifery Council, government agencies such as the Child Support Agency). You should seek confirmation of any such power before disclosing personal data in response to a request. If you need guidance, please contact the Data Protection Officer Mr Leigh Albrecht.

Further, without a warrant, the police have no automatic right of access to records of personal data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders. You should seek written assurances from the police that the relevant exemption applies. If you need guidance, please contact the Data Protection Officer Mr Leigh Albrecht.

Some additional sharing of personal data for research purposes may also be permissible, subject to certain safeguards.

Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, *Paritas Recruitment* will disclose requested data. However, the DPO will ensure the request is legitimate, seeking assistance from the company's legal advisers where necessary.

Changes to this Policy

We reserve the right to change this policy at any time without notice to you so please check regularly to obtain the latest copy.