jpr / Institute for Jewish Policy Research

GDPR Policy

1.0 Overview

The Institute for Jewish Policy Research (JPR) is committed to protecting the rights, freedoms and privacy of individuals in accordance with the General Data Protection Regulation (GDPR).

2.0 Purpose

The GDPR became legally enforceable on 25th May 2018 and applies to individuals and organisations operating within the EU. The regulation places specific legal obligations on data controllers and data processors with regards to the handling of personal data. As a processor, JPR is legally required to take certain steps to protect personal information in its care. JPR will have a legal liability if the organisation is responsible for a breach.

This document outlines how JPR intends to comply with the requirements of the GDPR.

3.0 Scope

This policy applies to all personal data processed and controlled by JPR. The policy is available to all staff and volunteers working with JPR. This includes all temporary or locum staff, and agents acting on behalf of JPR.

While voluntary, temporary and locum staff are expected to comply with the policy, this does not imply or create an employment relationship.

A copy of this policy will also be made available on the JPR website.

4.0 Compliance

Any breach of this policy or the regulation itself will be considered an offence and will be dealt with under JPR disciplinary procedures.

Breaches of the regulation will be reported to the Information Commissioners Office (ICO).

5.0 Policy

The GDPR demands higher transparency and accountability for the handling of personal data. JPR needs to process specific information about its employees, subscribers, donors and other stakeholders for various reasons such as, but not limited to:

- Paying staff and keeping internal records
- Communicating information it produces
- Tracking website visitors
- Raising funds
- Complying with legal obligations

The GDPR applies to both ‘controllers’ and ‘processors’. The data controller determines the purposes and means of processing personal data. The data processor is responsible for processing personal data on behalf of a controller.

To comply with the GDPR, JPR must ensure that the data it collects are processed fairly, collected for legitimate reasons, adequate for their purpose, accurate and up to date, deleted when no longer needed, and processed and stored securely. The organisation is committed to demonstrating how it is taking steps to comply with these principles.

5.1 What are Personal data?

The GDPR defines personal data as any information that relates to an identifiable person who can be identified, directly or indirectly, from that information (the Data Subject).

Personal data can include:

- Names
- Dates of birth
- Location data
- Email addresses
- Addresses
- Identification numbers
- IP addresses
- Pseudonymous data
- Online identifiers

5.2 What is Sensitive Personal Data?

The GDPR refers to sensitive personal data as “special categories of personal data”.

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Sensitive Personal Data can include data about:

- Health
- Genetics
- Biometrics
- Sexual orientation
- Trade union membership
- Political opinions or beliefs
- Religious or philosophical beliefs

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

Where JPR processes Sensitive Personal Data, they will be anonymised. Sensitive Personal Data are primarily processed for research purposes in relation to the organisation’s core activities.

5.3 Principles

Article 5 of the GDPR requires that personal data shall be:

“a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, 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;

e) kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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.”

Article 5 (2) requires that:

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

JPR intends to comply with the above requirements and will implement appropriate mechanisms to ensure continued compliance.

5.4 Types of data JPR may process

JPR has defined that the following data categories may be collected, processed and used:

- ☐ Employee/Volunteer/Part Time Workers Name, Title, Address, Contact Details, Staff Numbers, Payroll Numbers
- ☐ Personal, professional, commercial or business addresses
- ☐ Date / Year / Birth Date
- ☐ Telecommunications data (e. g. connection, location, usage and traffic data)
- ☐ Telephone Numbers
- ☐ Email Address
- ☐ Third Party Data for the purposes of communication and liaison between JPR and third parties

- ☐ Contract data (contractual relationship, product and/or contractual interests)
- ☐ Payment data
- ☐ Personal data that are covered by the obligation to maintain professional secrecy
- ☐ IP addresses
- ☐ Planning and control data
- ☐ Cookies

5.5 Categories of Data Subjects

JPR has defined the following data subject categories from whom the Personal Data as defined above may be collected, processed and used:

- ☐ Employees (Internal)
- ☐ Contact persons
- ☐ Employees of external companies
- ☐ Interested parties
- ☐ Tenants / landlords, lessees / lessors
- ☐ Suppliers

5.6 Lawful bases for Processing

What are the lawful bases for processing?

The lawful bases for processing are set out in Article 6 of the GDPR. JPR will identify the lawful bases for processing wherever the organisation processes data. The lawful bases for processing are as follows:

"(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests."

Source: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

5.7 Consent

Where consent is relied upon as a legal basis for processing, JPR will collect consent in a recorded and demonstrable manner. Consent will be gathered in a way that is freely given, specific, informed and unambiguous. JPR will make it explicitly clear to the individual what they are giving consent for, and will process their personal data in a manner that is consistent with the consent the individual has given. JPR will make it as easy for an individual to revoke consent as it was to grant consent.

Marketing emails sent by JPR will include an unsubscribe link.

5.8 Controllers and Processors

As a Data Controller, JPR will only work with processors who can provide sufficient guarantees to implement appropriate technical and organisational safeguards to meet the GDPR requirements and protect the rights, freedoms and privacy of Data Subjects.

As a Data Controller and Processor, JPR will implement its own appropriate technical and organisational safeguards where the organisation processes data to ensure the rights, freedoms and privacy of Data Subjects. Where the organisation processes sensitive personal data, additional safeguards will be implemented.

JPR will implement:

- pseudonymisation and/or encryption of personal data where required;
- measures to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data;
- measures to ensure the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- appropriate policies and governance frameworks to ensure continued compliance throughout the organisation.

All controller-processor relationships will be documented and managed with contracts that mandate privacy obligations.

5.9 Responsibilities

JPR will assign appropriate GDPR and Data Protection responsibilities to its staff. Staff who are made responsible for GDPR and Data Protection will be given sufficient support and resources to fulfil their responsibilities. The organisation may appoint a dedicated Data Protection Officer (DPO) in future.

The staff who are made responsible for GDPR and Data Protection will:

- inform and advise stakeholders, including staff, volunteers and other parties as relevant, of their obligations to comply with the GDPR and other applicable laws;
- monitor compliance with the GDPR on an ongoing basis;

- issue appropriate training to staff involved with data processing;
- ensure appropriate resources are made available for GDPR and Data Protection considerations;
- conduct data impact assessments when required;
- work with the relevant supervisory authorities on issues relating to the processing of personal data;
- implement appropriate measures to be able to evidence compliance with GDPR.

All staff, volunteers or locum employees working at JPR will be responsible for maintaining an awareness of the requirements of the GDPR and for seeking appropriate assistance when processing personal data.

5.10 Technical and organisational measures based on the EU General Data Protection Regulation

JPR will implement appropriate technical and organisational measures to protect personal data against accidental loss, alteration, disclosure or access. These measures ensure a level of security appropriate to the risks presented by the processing and the nature of personal data being processed.

JPR ensures that the processing of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law and does not violate the relevant provisions.

JPR has implemented, but not limited to, the following measures to prevent the unauthorised access to data processing systems where personal data is processed:

☒ Alarm system	☒ CCTV at entry points (all entrances)
☒ Access control policies	☒ Security locks
☒ Photoelectric sensors / Movement detectors	☒ Security staff
☒ Key management (Issuance of keys, etc.)	☒ Visitor management at reception desks
☒ Logging of visitors	☒ Careful selection of cleaning staff
☒ Careful selection of security mechanisms	
☒ Manual locking system (Limited usage for key employees to be used in the event of a failure in the access control systems	

Access Control (systems)

JPR has implemented, but not limited to, the following measures, to prevent the use of data processing systems by unauthorised persons:

☒ Assignment of user rights	☒ Assignment of user profiles to IT systems
☒ Assignment of passwords	☒ Encryption and/or password protection or touch-ID for mobile storage media
☒ Authentication with username / password	☒ Encryption and/or password protection or touch-ID on laptops / notebooks
☒ Use of Intrusion-Prevention-Systems	☒ Use of a software firewall (office clients)
☒ Use of hardware firewalls	
☒ Creation of user profiles	
☒ Additional measures: web-application	

firewalls, regular vulnerability scans, regular penetration testing, patch management, minimum requirements for password complexity and forced password changes, use of virus scanners	

Access control (data)

JPR has implemented, but not limited to, the following measures, to ensure that authorised users of a data processing system may only access the data for which they are authorised, and to prevent personal data from being read while the data are in use, in motion, or at rest without authorisation:

☒ Creation of an authorization concept	☒ Disk encryption (backup tapes for off-site storage, laptops)
☒ Number of administrators reduced to "absolute necessary"	☒ Management of rights by system administrators
☒ Logging of application access, especially during the entry, modification and deletion of data	☒ Password policy including password length, password change management
☒ Secure media sanitisation	☒ Secure storage of data carriers
☒ Use of shredders	☒ Logging of secure media destruction
	☒ Compliant destruction of data media

Transfer control

JPR has implemented, but not limited to, the following measures, to ensure that personal data cannot be read, copied or modified during electronic transmission or during transportation or storage to disk. Additionally, to control and determine to which bodies the transfer of personal data provided by data communication equipment is allowed:

☒ Documentation of recipients of data and the time periods for the provision of data including agreed deletion times	☒ Disclosure of data in anonymous or pseudonymous form
☒ During physical transport, careful selection of transport personnel and vehicles	☒ Creation of an overview of regular request and delivery operations
☒ Disk encryption	

Input control

JPR has implemented, but not limited to, the following measures, to ensure that it is possible to subsequently control, and determine if and by whom, personal data have been entered, changed or removed on data processing systems:

☒ Logging of input, modification and deletion of data	☒ Creation of an overview of which applications are permitted to input, modify or delete which data
☒ Traceability of input, modification and deletion of data by individual user names (not user groups)	

☒ Granting of rights for the input, modification or the deletion of data based on an authorisation concept

Order control

JPR has implemented, but not limited to, the following measures, to ensure that personal data which are processed by request of the data owner by a data processor, shall only be processed as instructed by the data owner:

☒ Contractor selection via history review (in particular regarding data security)
☒ Written instructions to the contractor (for example, by Data Processing Agreement) (GPDR)
☒ Ensure contractors have appointed Data Protection Officers
☒ Effective control rights over data processors have been agreed
☒ Prior examination of the documentation and the security measures taken by the contractor
☒ Obligation of the contractor's employees to maintain data confidentiality (GPDR)
☒ Ensure the secure destruction of data after termination of the contract
☒ Continual review of contractors and their activities

Availability control

JPR has implemented, but not limited to, the following measures, to ensure that personal data are protected against accidental destruction or loss:

☒ Fire and smoke detection systems
☒ Alarm when unauthorised entry is detected
☒ Testing of data recovery
☒ Secure off-site storage of data backups
☒ Protection power strips
☒ Fire extinguishers
☒ Creation of a backup & recovery concept
☒ Preparation of an emergency response plan

5.11 Data Subject Rights

Individuals (Data Subjects) have certain rights in relation to their personal data under the GDPR. Those rights include;

- **The right to be informed** - Data Subjects have a legal right to confirm whether or not their personal data are being processed and to access those data along with certain additional information.

- **The right of access** – Data Subjects have a legal right to access a copy of the personal information held about them. This must be supplied in a commonly used format (e.g. PDF, Excel or Word document).

- **The right to rectification** – Data Subjects have the right to have any inaccurate personal data rectified and, taking into account the purposes of the processing, to have any incomplete personal data completed.

- **The right to erasure** – In some instances, Data Subjects have a right to

request the erasure of their personal data without delay. These instances may include: processing is no longer necessary; consent has been withdrawn where the legal basis for processing is consent; the Data Subject objects to processing and there is a valid reason under Data Protection law; processing is for direct marketing purposes, and the data have been unlawfully processed. General exclusions from this clause may include where processing is necessary for a legal reason or for the exercise or defence of legal claims.

- **The right to restrict processing** – In some instances Data Subjects have a right to restrict the processing of their personal data. These instances include: the data are inaccurate; processing is unlawful but the subject opposes erasure; the subject has objected to certain forms of processing but agrees to other forms, or the subject objects to processing but the organisation requires it for the exercise or defence of legal claims.

- **The right to data portability** – The right to data portability gives individuals the right to receive personal data they have provided in a structured, commonly used and machine-readable format. It also gives them the right to request that their data are transferred from one controller to another.

- **The right to object** – Article 21 of the GDPR gives individuals the right to object to the processing of their personal data. The right to object only applies in certain circumstances. Whether it applies depends on the purpose for processing and the lawful basis for processing. Individuals have an absolute right to object to data processing for direct marketing purposes.

- **Rights in relation to automated decision making and profiling** – Individuals have the right not to be subject to the results of automated decision making, including profiling, which produces legal effects on them or otherwise significantly affects them. This is defined as a process where there is no human involvement in the decision-making process.

JPR intends to comply with the above rights of individuals and will not take part in automated decision-making and profiling activities.

JPR will make all reasonable efforts to ensure that individuals who are the focus of the personal data (Data Subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

JPR will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual is informed of any additional processing before it takes place.

JPR will not seek to collect any personal data which are not strictly necessary for the purpose for which they were obtained. Forms for collecting data will always be

drafted with this in mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

JPR will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that these are accurate, and each individual should notify JPR if, for example, a change in circumstances means that the data need to be updated. It is the responsibility of JPR to ensure that any notification regarding the change is noted and acted on.

JPR undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means JPR will undertake a regular review of the information held and implement a weeding process.

JPR will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

Where consent is relied on as a lawful basis for processing at JPR, individuals have a right to withdraw consent at any time.

5.12 Data retention and deletion

JPR will not retain or process Personal Data for longer than is necessary or for longer than any period agreed to by the Data Subject. As a general rule, data will be retained as long as a relationship exists between the organisation and the Data Subject, plus a maximum of 6 years.

JPR agrees to return or destroy the Data Subjects data if the Data Subject requests for the organisation to do so. Following the deletion of Personal Data JPR shall notify the Data Subject that the Personal Data in question have been deleted. Where applicable, the Processor shall also provide confirmation that the Personal Data have been destroyed in accordance with instructions issued by the Data Subject.

5.13 Location of processing

All data processed by JPR will be processed within the European Economic Area (EEA).

5.14 Transfers outside the European Economic Area

JPR will not transfer personal data to territories outside of the European Economic Area (EEA) without the explicit consent of the individual.

This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - JPR will always seek the consent of individuals before placing any personal data (including photographs) on its website.

5.15 Record keeping

In addition to the above actions, JPR commits to keeping appropriate records for the purpose of demonstrating compliance with the GDPR.

6.0 Subject Access Requests (Data Subject Access Requests/DSARs)

If individuals believe that JPR is processing data about them, they may request a copy of their personal data. This will be provided in a commonly used format. **JPR reserves the right under the GDPR to charge a reasonable fee to cover administration costs where Subject Access Requests are manifestly unfounded or excessive**. In this event, JPR will delay the release of data until the fee is paid in full. JPR will comply with Subject Access Requests within 30 days of receipt.

Subject access requests should be directed in writing to:

Post: Data Protection, The Institute for Jewish Policy Research (JPR), ORT House, 126 Albert Street, London, NW1 7NE

Email: jpr@jpr.org.uk

7.0 Breach & notification

In the event of a breach involving personal data, JPR will notify the Information Commissioners Office (iCO) promptly and without undue delay. Where feasible, the ICO will be notified no later than 72 hours after the organisation becomes aware of the breach. Where this timeframe cannot be met, JPR will provide a reasoned justification for the delay.

Notice is not required if the breach is unlikely to result in a risk to the rights and freedoms of individuals.

If an individual believes that JPR's processing activities infringe data protection laws, the individual has a legal right to lodge a complaint with a relevant supervisory body. In the United Kingdom the governing body is the Information Commissioners Office (the ICO). You can find their details online: https://ico.org.uk

8.0 Penalties

Regulators have authority under the GDPR to issue penalties equal to the greater of €10 million or 2% of the entity's global gross revenue for violations of record-keeping, security, breach notification, and privacy impact assessment obligations.

Violations of obligations related to legal justification for processing, Data Subject rights, and cross-border data transfers may result in penalties of the greater of €20 million or 4% of the entity's global gross revenue.

9.0 Applicability of other policies

This document is part of JPR's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such, the applicable policies should be reviewed as needed.

Recommended further reading:

- Acceptable Use of IT Assets Policy
- Access Control Policy
- Confidentiality Policy
- Data Retention Policy
- Disaster Recovery Policy
- Incident & Data Breach Response Policy
- Incident Report Form
- Information Security Policy
- Mobile Device Policy
- Password Policy
- Privacy & Cookie Policy
- Remote Access Policy
- Wireless Policy

10.0 Document review

This policy will be reviewed at least annually and approved by the senior management team at JPR.

11.0 Contact information:

Please direct all queries to:

Data Protection
JPR / Institute for Jewish Policy Research
ORT House
126 Albert Street
London
NW1 7NE

tel. +44 (0)20 7424 9265
email: jpr@jpr.org.uk

The Institute for Jewish Policy Research (JPR) is a registered charity (no. 252626) and company limited by guarantee (registration no. 00894309 London), registered office as above.