

## Privacy and Cookie Policy

The Institute for Jewish Policy Research is hereinafter referred to as JPR and “the organisation”. In this policy, “we”, “us” and “our” refer to JPR, the owner and operator of this website.

### 1.0 Introduction

JPR is committed to respecting the rights, freedoms and privacy of the individuals who visit our website. This policy applies where JPR processes the personal data of website visitors.

The General Data Protection Regulation (GDPR) places particular emphasis on protecting personal data. Personal data means information that relates to an identifiable individual. In short, if a living individual can be identified from a piece of information it is classified as personal data. This includes website Cookies and IP addresses.

While many types of data require some degree of protection, this policy is primarily aimed at data that could cause harm if incorrectly handled, particularly personal data.

Examples of personal data include:

- Names
- Email addresses
- Home addresses
- Work addresses
- Dates of birth
- Telephone numbers
- Biometric data
- Health data
- IP addresses
- Cookies

This is not an exhaustive list.

### 2.0 Scope

This policy applies to the JPR website and the information collected via any website owned and operated by JPR.

### 3.0 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.

#### 4.0 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 is 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 has 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.

## **5.0 Information we collect**

We collect specific information on our website. The type of data we collect depends on how you use this website. We collect the following types of information:

Anonymous data such as cookies. We may process data about your use of our website (“this is defined as usage data”). Usage data can include your IP address, geographical location, the browser and version you use, your operating systems, where your visit came from (referral source), the length of your visit, the pages you view, your visit navigation path, information about the timing, frequency and pattern of your website visits. The usage data may include your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of your website visits. This information is collected automatically by programmes such as Google Analytics.

This information is used for the purposes of analysis. We use this information to track the volume of visits to our website and to analyse how our website is performing. We use this information to understand who is visiting our website, for how long visitors stay on the site, and to understand which pages are popular and which are not. We use this information to make improvements to our website and to analyse the performance of staff who are responsible for maintaining the website and producing content. This information is not used for any other purposes.

The lawful basis for this processing is our legitimate interest, namely monitoring and improving our website and services.

Personal data such as names, email addresses, addresses, telephone numbers, job titles and employment details. This information is collected from website visitors when they submit the data to our website, for example, when they subscribe to our mailing list or submit an enquiry. We use this information to send newsletters and information about JPR where a visitor has asked us to do so, or to respond to enquiries that arrive through our website.

The lawful basis for this processing is consent, legitimate interests and legal obligations, namely consent for marketing communications and the proper management of our relationships.

In addition to the purposes above, we may process your personal data where processing is necessary for compliance with a legal obligation, a public task, or in order to protect your vital interests or that of another person. Information may be used where necessary for the

establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative out of court procedure. Information may also be used for the purposes of risk management or to obtain professional advice where it is in our legitimate interests to do so.

## **6.0 About cookies**

Cookies are small files that are placed on your computer by websites you visit. They are used to make websites work efficiently as well as to provide information to the owner or operator of a website.

Cookies are either “persistent” or “session” cookies. Persistent cookies are stored and remain valid until they expire, whereas a session cookie will expire at the end of the website visit, when the browser is closed. In both cases, the cookie will cease to exist if it is deleted.

The cookies we collect do not typically contain personal data, but other information we collect about you may be linked to the information stored in cookies.

If you wish to disable cookies, we encourage you to do so within your website browser privacy settings. However, certain parts of our website may not function correctly if cookies are disabled.

For more information, including how to disable cookies, please visit <https://www.aboutcookies.org>.

## **7.0 Subscribing**

Where information is submitted for the purpose of subscribing to our mailing list, our newsletter will be sent to the email address provided. There will be a clear unsubscribe option in each newsletter we send. We kindly request that you do not submit another individual's details to our website without their express permission.

## **8.0 Disclosing your information**

Your information will not be disclosed to any organisation or person outside JPR without your express permission, unless there is a legal reason for JPR to disclose your data.

## **9.0 International transfers**

Any information we collect or that you provide to us will be processed within the European Economic Area (EEA). Your information will not be transferred outside the EEA but may be stored on cloud servers based outside the EEA. In such circumstances, the information will be password protected, encrypted and stored by a provider who provides adequate assurance of compliance with the relevant legal obligations. For example, they will be covered by EU-US Privacy Shield or a similar arrangement.

### **10.0 Retaining and deleting personal data**

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.

### **11.0 Data destruction**

Data destruction is a critical component of a data retention policy. Data destruction ensures that information is deleted in a secure and efficient manner.

When the retention timeframe expires, JPR will actively destroy the data covered by this policy. Every attempt will be made to delete all duplicate information simultaneously.

### **12.0 Subject Access Requests (Data Subject Access Requests/DSARs)**

If individuals believe that JPR is processing data about them, they are free to request a copy of their personal data. This will be provided in a commonly used format. JPR will charge a £10 fee to cover administration costs. JPR will comply with all 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), 6 Greenland Place, London, NW1 0AP

Email: [jpr@jpr.org.uk](mailto:jpr@jpr.org.uk)

### **13.0 Breach & notification**

The Information Commissioners Office (the ICO) is the governing body responsible for enforcing the GDPR in the United Kingdom. In the event of a breach involving personal data, JPR will notify the 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>

#### **14.0 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.

#### **15.0 Document review**

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

#### **16.0 Contact information:**

Please direct all queries to:

**Data Protection**

JPR / Institute for Jewish Policy Research  
6 Greenland Place  
London  
NW1 0AP

tel. +44 (0)20 7424 9265

email: [jpr@jpr.org.uk](mailto: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.