JPPC
CHARTERED TOWN PLANNERS

Privacy And Personal Data Protection Policy

Contents

1. Introduction

In its everyday business operations JPPC makes use of a variety of data about identifiable individuals, including data about:

- Current, past and prospective employees;
- Clients;
- Suppliers including Potential Suppliers;
- Users of its website;
- Subscribers;
- Other stakeholders.

In collecting and using this data, the organisation is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps company name is taking to ensure that it complies with it.

This control applies to all system, people and processes that constitute the organisation's information systems, including board members, directors, partners, employees, supplies and other third parties who have access to the organisation's systems.

The following policies and procedures are relevant to this document:

- Data Protection Impact Assessment Process
- Personal Data Mapping Procedure
- Legitimate Interest Assessment Procedure
- Information Security Incident Response Procedure
- Records Retention and Protection Policy

2. Privacy And Personal Data Protection Policy

2.1. The General Data Protection Regulation

The General Data Protection Regulation (GDPR) is one of the most signification pieces of legislation affecting the way that JPPC carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of the European Union. It is company name's policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.

2.2. Definitions

There are a total of 26 definitions listed within the GDPR. The most fundamental definitions with respect to this policy are as follows:

Personal Data – is defined as any information relating to an identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to and identifier such as 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.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment of combination, restriction, erasure or destruction.

Controller – means the natural or legal person. Public authority, agency or other body which, alone or jointly with others, determines the purposes and means of such processing are determined by Union or Member State Law, the controller or the specific criteria for its nomination may be provided for by Union or Member State Law.

2.3. Principles Relating To Processing Of Personal Data

There are a number of fundamental principles up on which the GDPR is based. These are as follows:

1. Personal data shall be:
    a. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
    b. Collected for specified, explicit and legitimate purposed 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 purposed or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
    c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
    d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
    e. Kept in a form which permits identification of data subject for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer period insofar as the personal data will be processed solely for archiving purposed in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
    f. Processed in a manner that ensure 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 ('integrity and confidentiality').
2. The Controllers shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

The organisation must ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing e.g. new IT systems.

2.4. Rights Of The Individual

The data subject also has rights under the GDPR. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights must be supported by appropriate procedures within JPPC that allow the required action to be taken within the timescales stated in the GDPR.

The timescales are shown below:

Data Subject Request	Timescale
The right to be informed	When data is collected (if supplied by data subject) or within one months (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objections
Rights in relation to automated decision making and profiling	Not specified

2.5. Lawfulness Of Processing

There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under GDPR. It is company name Thomson and Partners LLP policy to identify the appropriate basis for processing and to document it, in accordance with the Regulation. The options are described in brief below:

2.5.1 Consent

Unless it is necessary for a reason allowable in the GDPR, explicit consent must be obtained from a data subject to collect and process their data. In the case of children below the age of 16 parental consent must be obtained (a lower age may be allowed in specific EU member states). Transparent information about your usage of their personal data must be provided to data subjects at the time that consent is obtained and their rights with regards to their data explained, such as the right to withdraw consent. This information must be provided in an accessible form, written in clear language and free of charge.

If the personal data is not obtained directly from the data subject then this information will be provided within a reasonable period after the data is obtained and definitely within one month.

2.5.2 Performance Of Contract

Where the personal data collected and processed is required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question e.eg. a delivery/service cannot be made/provided without an address to deliver to.

2.5.3 Legal Obligation

If the personal data is required to be collect and processed in order to comply with the law, then explicit consent is not required. This may be the case for some data relating to employment and taxation for example, and for many areas addressed by the public sector.

2.5.4 Vital Interests Of Data Subject

In a case where personal data is required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. The organisation will retain reasonable, documented evidence that this is the case, whenever this reason issued as the lawful basis of the processing of personal data. As an example, this may be used in aspects of social care, particularly in the public sector.

2.5.5 Tasks Carried Out In The Public Interest

Where the organisation needs to perform a task that it believes is in the public interest or as part of an official duty then the data subject's consent will not be requested. The assessment of public interest of official duty will be documented and made available as evidence when required.

2.5.6 Legitimate Interests

If the processing of specific, personal data is in the legitimate interests of JPPC and is judged not to affect the rights and freedom of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this will be documented.

2.6. Privacy By Design

JPPC has adopted the principle of privacy by designing and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

The data protection impact assessment in include:

- Consideration of how personal data will be processed and for what purposes
- Assessment of whether the prosed processing of personal data is both necessary and proportionate to the purpose(s)
- Assessment of the risks to individuals in processing the personal data

- What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimisation and pseudonymisation should be considered where applicable and appropriate.

2.7. Contracts Involving The Processing Of Personal Data

JPPC will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by GDPR.

2.8. International Transfer Of Personal Data

Transfer of personal data outside the EU will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the EU's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

Intra-group international data transfers will be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

2.9. Data Protection Officer

A defined role of Data Protection Officer (DPO) is required under GDPR if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or an outsourced to an appropriate service provider.

Based on this criteria, JPPC does not require a DPO to be appointed.

2.10. Breach Notification

It is JPPC's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance with our ***Information Security Incident Response Procedure*** which sets out the overall process of handling information security incidents.

2.11. Addressing Compliance To The GDPR

The following actions are undertaken to ensure that JPPC complies at all times with the accountability principle of GDPR:

- The legal basis for processing personal data is clear and unambiguous
- A Data Protection Officer is appointed with specific responsibility for data protection in the organisation (if applicable)
- All staff involved in handling personal data understand their responsibilities for following good data protection practice

- Training in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving personal data are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
    - Organisation name and relevant details
    - Purposed of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreement and mechanisms for transfers of personal data to non-EU countries including details of controls in place
    - Personal data retention schedules
    - Relevant technical and organisational controls in place

These actions will be reviewed on a regular basis as part of the management process concerned with data protection.

2.12. Our Obligations To Our Suppliers And Potential Suppliers

The organisation will process personal data to aid the purchasing of goods/services provided by a supplier.

When the organisation is provide with a service/product, the supplier will be asked to provide the organisation with information about the company and certain personal information (i.e. contact information for key personnel) during the supplier registration process.

This personal data will be collect, stored and used to contact the supplier, when the organisation has a requirement for the supplier's goods and/or service.

Access to personal data will be restricted to the organisation's employees and designated third party agents who have a need to know the specific information in question in order to carry out their responsibilities with regards to the organisation's procurement process. The supplier will be notified if any personal data will be passed onto third parties and the supplier will have the opportunity to refuse that this is undertaken.

The organisation will retain the supplier data for six years after the final supply date, to comply with accounting regulations. Once the archiving period has come to an end, the data will then be destroyed by being deleted and shredded/incinerated.

In the event that a business relationship with the organisation is not established, the organisation will retain the personal data for a period of up to 6 months, unless notified by the supplier requesting that it is destroyed sooner. The data will then be destroyed by being deleted and shredded/incinerated.

This policy does not constitute a contract between the organisation and any supplier or potential supplier.

3. Revision History

Version	Date	Revision Author	Summary Of Changes
1	May 2018		Implementation