EDGE IT Systems Ltd

GDPR Policy

GDPR Policy

1. Version history details and author

1.0	02/10/2018	Creation	C.EDGE
2.0	16/01/2023	Review of policy & modification to section 4 (spelling error)	S.PELCHAT

2. Introduction

EDGE IT Systems Limited (hereinafter referred to as 'We' or 'we') is determined to protect the rights and freedoms of data subjects with regard to their personal data. We are also committed to facilitating the exercise of data subject rights over their data. This document lays out our policy, but also demonstrates our intent.

3. Data Protection by Design and Default

When creating or modifying systems and procedures for processing personal data, we will consider the protection of personal data. We will ensure we collect no more data attributes than we need, and we will keep the data for only as long as we need it. If we intend to process personal data which is likely to result in a high risk to the data subject, we will conduct a Data Protection Impact Assessment. We will consult with the ICO where the Data Protection Impact Assessment indicates processing will result in a high risk to data subjects. We will only process data within the UK or EU.

4. Say what we do and do what we say

We will tell data subjects what data we hold about them, how and why we will process it, and inform them of their rights concerning their personal data. We will not mislead data subjects about processing. We will only process personal data in the ways we have told data subjects.

5. Data Accuracy

The data subject has a right to request rectification, but we will also make our best efforts to ensure the personal data is accurate. When we become aware that personal data is inaccurate, we will try to update it. Where this is not possible, we will stop processing the data. When personal data changes we will inform any recipients of that data of the changes.

6. Information Security Concerning Personal Data

We shall assess the risks of processing to the data subject and will deploy appropriate security measures. To ensure security, where appropriate, we will:

- train our team members to understand personal data is important and must be treated correctly
- control access to the personal data using authentication and authorisation, to keep it confidential
- keep backups to help us guard against loss and damage
- ensure the personal data is available when and where it is required
- only use operating systems and software that receive security patches
- install security patches as they become available
- keep up to date with current advice and changes in the risk landscape

7. Data Subject Rights

We are committed to respecting and facilitating the exercise of data subject rights. We will train our staff to recognise requests from data subjects and will create procedures to satisfy the exercise of those rights. We will ensure we are transparent about why and how we process personal data.

Right to Access

When access is requested, where possible, we will:

- check the identity of the data subject before releasing personal data to them
- protect the rights of other natural persons while fulfilling a data subject access request
- explain the processing and the categories of personal data being processed
- respond to data subject access requests within 30 days

If it is not possible to provide access, we will tell the data subject.

Right to Rectification

When rectification is requested, where possible, we will:

- correct personal data without delay
- complete incomplete personal data
- add extra information in the form of notes
- notify any recipient of the personal data of the rectification

If it is not possible to rectify the personal data, we will tell the data subject.

Right to Erasure

When erasure is requested, where possible, we will:

- erase the personal data without delay
- notify any recipient of the personal data of the erasure

If it is not possible to erase the personal data, we will tell the data subject.

We may keep enough personal data to ensure we do not direct market to the data subject again. This data will be kept on the basis of having a 'legal obligation' to do so.

Right to Restriction of Processing

When a restriction of processing is requested, where possible, we will:

- temporarily restrict processing of the personal data without delay
- notify the data subject before we lift the restriction
- only process restricted personal data with the explicit consent of the data subject
- notify any recipient of the personal data of the restriction of processing

If it is not possible to restrict processing of the personal data, we will tell the data subject.

Data Subject Rights (continued …)

Right to Data Portability

When we receive a request for data portability, where possible, we will:

- check the identity of the data subject before releasing personal data to them
- protect the rights of other natural persons while fulfilling a data portability request
- provide the data in CSV form without delay

If it is not possible to provide data portability, we will tell the data subject.

Right to Object

- When an objection to data processing, where possible, we will stop processing of the personal data without delay

If it is not possible to stop processing of the personal data, we will tell the data subject.

We may keep enough personal data to ensure we do not direct market to the data subject again. This data will be kept on the basis of having a 'legal obligation' to do so.

Automated individual decision making, including profiling

We do not perform automated individual decision making, or profiling. If we ever need to, this will be considered as part of the requirements of the new process.

8. Transfers

We will be responsible about transferring personal data to other controllers and processors. When using processors, the processing will be governed by a written contract. When transferring personal data to other controllers we will take reasonable steps to ascertain their identity, and ensure they will respect and protect the rights and freedoms of the data subjects, including introducing contractual terms.

We will not transfer data outside the EU or to an international organisation unless:

- there is an adequacy decision made by the EC
- the transfer is covered by binding corporate rules

9. Cooperation with the ICO

We will cooperate with the ICO on any personal data protection issues.

10. Personal Data Breach Detection

We will take appropriate measures to detect a personal data breach.

11. Personal Data Breach Notification

If we become aware of a personal data breach we will without delay:

- investigate the cause of the data breach
- identify the number of personal data records affected
- assess the risks to the rights and freedoms of data subjects
- inform the ICO of the personal data breach within 72 hours

If the personal data breach is deemed likely to result in a high risk to the rights and freedoms of data subjects, we will seek guidance from the ICO. We are prepared to notify the data subjects affected, if practicable. If this is not practicable, we will notify data subjects by making a public announcement, such as through the national news media.

12. Websites and On-line Services

We will ensure data subjects are informed about how their personal data will be used, when it is captured through our websites.

We will ensure the documentation on our websites is clear and easy to understand by the intended audience.

13. Children

We believe children should be afforded additional protection. We will ensure all communications intended for an audience of children will be written in an appropriate way so that children can understand and make informed decisions about their personal data.

Where appropriate we will seek confirmation from a holder of parental responsibility.