Data Protection (GDPR) Policy

Prepared by: David J. Black

Prepared for: Mike Brown

Date: May 2018

Issue: V2.0

PUBLIC

QA Ltd
Rath House
55-65 Uxbridge Road
Slough
SL1 1SG

Tel: +44 (0) 1753 898 300
Fax: +44 (0) 1753 898 305
Web: www.qa.com

Contents Page

2 Data Protection Principles & Policy

The GDPR principles are defined by EU law, and managed within the UK by the Information Office (ICO) and form the fundamental principles which must be considered when handling all elements of data.

It is vital that all users understand the importance of protecting personal data and they are familiar with this policy, and that they put its security procedures into practice.

All users must ensure they are aware of the following:

s duties under the GDPR and restrictions on the use of personal data, detailed within this document;

the responsibilities of all users for protecting personal data, including the possibility that they may commit criminal offences if they deliberately try to access, or to disclose, information without authority;

the dangers of people trying to obtain personal data by deception (for example, by pretending

persuading you to alter information when you should not do so;

any restrictions QA places on the personal use of its computers and IT systems by staff (to avoid, for example, virus infection or spam).

2.1 Lawfulness, fairness and transparency

The first GDPR principle states You must have a valid lawful basis in order to process personal data.

In practice, it means that you must consider:

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

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

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

Vital interests:

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.

4ßW0ßx

securely delete information that is no longer needed for this purpose or these purposes; and

update, archive or securely delete information if it goes out of date or has reached the end of the retention period;

Ensure that the data subject is aware how long we will retain their data.

2.6 Integrity and confidentiality

processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

In practice, it means QA must have appropriate security to prevent the personal data we hold being accidentally or deliberately corrupted or compromised.

In particular, QA needs to:

design and organise our security to fit the nature of the personal data QA hold and the harm that may result from a security breach;

be clear about who within QA is responsible for ensuring information security for each element of data we process;

make sure QA have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff;

be ready to respond to any breach of security swiftly and effectively.

appropriate for QA depend on each circumstance, so you should adopt a risk-based approach to deciding what level of security QA need to implement.

It is important to understand that the requirements of the GDPR go beyond the way information is stored or transmitted.

Every security measure put in place must ensure that:

only authorised people can access, alter, disclose or destroy personal data;

those people only act within the scope of their authority;

if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned;

it is appropriate to the nature of the information in question;

it is commensurate to the harm that might result from its improper use, or from its accidental loss or destruction.

Physical and technological security is likely to be essential, but is unlikely to be sufficient in itself. Managerial, procedural and organisational security measures are likely to be equally important in protecting personal data.

2.7 Individual Rights

GDPR requires that the rights of all data subjects are considered when processing data.

In practice this means that i rights are comprised of:

The right to be informed

1.

Rights in relation to automated decision making and profiling.

1. The GDPR has provisions on:
    1. automated individual decision-making (making a decision solely by automated means without any human involvement); and
    2. profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.
2. The GDPR applies to all automated individual decision-making and profiling.
3. Article 22 of the GDPR has additional rules to protect individuals if you are carrying out solely automated decision-making that has legal or similarly significant effects on them.
4. QA can only carry out this type of decision-making where the decision is:
    1. necessary for the entry into or performance of a contract; or
    2. authorised by Union or Member state law applicable to the controller; or
    3.
5. QA must identify whether any of our processing includes automation of decisions or profiling and, if so, make sure that you:
    1. give individuals information about the processing;
    2. introduce simple ways for them to request human intervention or challenge a decision;
    3. carry out regular checks to make sure that systems are working as intended.

3 InfoSec, GDPR and Policy Breach

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

3.1 Incident Reporting

Should a breach of security, the GDPR or QA policy occur despite the measures QA have taken to secure data and other assets, it is important that QA deal with the breach quickly and effectively.

The GDPR requires that QA must also keep a record of any personal data breaches, regardless of whether QA are required to notify the Information Commissioners Office (ICO).

A data security breach can happen for a number of reasons:

access by an unauthorised third party;

3.3 Assessment of on-going Risk

Once the incident

4 Definitions

4.1 Data Controller

A person who either alone or jointly or in common with other persons determines the purposes for which and the manner in which any personal data are, or are to be, processed.

4.2 Data Subject

Any living individual who is the subject of the personal data.

4.3 Data Processor

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

4.4 Personal data

Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller.

As well as including obviously personal data such as names and addresses (including e-mail addresses), the definition inclu

sonal hobbies, or business activities, for example.

4.5 Sensitive Personal data

Sensitive personal data means personal data consisting of information as to -

race;

ethnic origin;

politics;

religion;

trade union membership;

genetics;

biometrics (where used for ID purposes);

health;

sex life; or

sexual orientation.

4.6 Recipient

Anyone who receives personal data, except the Data Controller, Data Subject, or Data Processor.

4.7 Third Party

Third party, in relation to personal data, means any person other than –

(a) the data subject,

(b) the data controller, or

(c) any data processor or other person authorised to process data for the data controller or processor.

4.8 Processing

Processing is defined as including but not limited to collection, storage, use, disclosure, or destruction of personal data.

4.9 Subject Access Request (SAR)

A Subject Access Request (SAR), as defined within the GDPR, is a request made by an individual to a company or body.

It is most often used by1 0 0 1 70.104 48(s)24(t)- 0 1 305.4 37.68 1(t)16( )]TJt1 0 0 1 (y)24( )-7(a)8(n)859054fct eaany c