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

Version Control

Document Information	
2.0	Updated in line with GDPR

Revision History			
Version	**Issue Date**	**Author**	**Description of Change**
0.6	Jan 2012	DJ Black	Issue to Mike Brown for comments
1.0	Jan 2012	DJ Black	Approved
1.1	Feb 2017	DJ Black	Approved
2.0	May 2018	DJ Black	Updated in line with GDPR

Document Approval		
Name	**Position**	**Viewed / Comments**
Mike Brown	IT Director	Approved
Mike Bansal	GDPR Project Manager	Approved

Please note:

Some narrative text within this document has been acquired from the Information Commissioners Office website. This is permitted under "Regulation 17 of the Re-use of Public Sector Information Regulations 2005". For further information, please visit http://www.ico.gov.uk.

Contents Page

1 Introduction

The purpose of this policy document is to communicate to users of QA systems as well as customers the approach and policies that QA adopts while processing data to ensure it complies with the requirements of the General Data Protection Regulation (GDPR). The GDPR is law, and not an optional set of guidelines – we are all responsible in our actions for ensuring that QA remains within the boundaries of the GDPR.

It is important to consider and fully understand the six principles (detailed within section 2 of this document) whenever we process data, as well as any additional specific client requested controls that may have been agreed within contractual terms.

If you are new to a customer account or are not aware of any client specific instructions, you should confirm with the relevant team leader or manager if any additional client specific controls have been agreed.

Everyone should be cognisant of the data they handle and process, from the point of consideration and awareness of the following:

- where does the data come from
- why do we need it
- does the subject know what we do with their data
- how do we process it
- do we have permission to process it
- how do we store it
- how do we secure it
- how do we ensure it is correct
- who has access to it
- how long do we retain it
- how do we dispose of it
- Do we have consent when we want to communicate with them

If, when considering the above points there are any doubts or concerns, the IT Service Desk should be contacted to gain a clear answer and understanding of the issue.

This policy document applies to all users, which include employees of QA, associates, apprentices, temporary staff, volunteers and employees of any partner organisations that are undertaking tasks (data processors) on QA's behalf.

Please refer to section 4 of this document for definitions of the terms used within this policy.

2 Data Protection Principles & Policy

The GDPR principles are defined by EU law, and managed within the UK by the Information Commissioner's Office (ICO) and form the fundamental principles of QA's policy 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:

- QA'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 to be the person whom the information is about or by making "phishing" attacks) or by 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 that "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:** the processing is necessary to protect someone's life.
- **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.
- **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. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Fairness generally requires you to be transparent – clear and open with individuals about how their information will be used. Transparency is always important, but especially so in many Marketing situations where individuals have a choice to grant or deny you their consent – and confirm whether they wish to enter into a relationship with you.

If individuals know at the outset what their information will be used for, they will be able to make an informed decision about whether to enter into a relationship or perhaps to try to renegotiate the terms of that relationship.

Assessing whether information is being processed fairly depends partly on how it is obtained. In particular, if anyone is deceived, misled or otherwise tricked when the information is obtained, then this is unlikely to be fair.

The GDPR sets a high standard for consent. But you often won't need consent. If consent is difficult, look for a different lawful basis.

Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.

.

- Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.
- Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent to processing a precondition of a service.

Legitimate interest is the most flexible lawful basis for processing, but you cannot assume it will always be the most appropriate. It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.

There are three elements to the legitimate interests basis. It helps to think of this as a three-part test. You need to:

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.

2.2 Purpose Limitation

The second GDPR principle states that data "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".

This means that QA must ensure that we only gather and process personal information for legitimate reasons – we cannot obtain data for one purpose and assume we can use it for any others without validating the decision and gaining the data subject's permission to do so.

In practice, the second data protection principle means that you must:

- be clear from the outset about why QA are collecting personal data and what we intend to do with each element of it;

2.3 Data Minimisation

The third GDPR principle states that data must be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;”

In practice, it means you must ensure that:

- QA only hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual; and
- We must know exactly why each element of data we gather is required and not gather more data than we actually need to complete the task.
- If there are stages in a process, you should only gather the data that you need during each stage. This is important where the future stages are not guaranteed to occur.

So you should identify the minimum amount of personal data QA need to properly fulfill the purpose. QA should hold that much information, but no more. This is part of the practice known as data minimisation.

2.4 Accuracy

The fourth GDPR principle states that data must be “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;”.

Although this principle sounds straightforward, the law recognises that it may not be practical to double-check the accuracy of every item of personal data QA receive. So the GDPR makes special provision about the accuracy of information that individuals provide about themselves, or that is obtained from third parties.

To comply with these provisions you should:

- take reasonable steps to ensure the accuracy of any personal data you obtain;
- ensure that the source of any personal data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to update the information.

2.5 Identification and Retention of data

The fifth GDPR principle states that data must be “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”.

GDPR does not set out any specific minimum or maximum periods for retaining personal data.

In practice, it means that QA need to:

- Ensure we can identify each data subject’s data and not mix it up with that of others.
- review the length of time QA keep each element of personal data;
- consider the purpose or purposes QA hold the information for in deciding whether (and for how long) to retain it;

- 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

The sixth GDPR principle states that “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.””.

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.

There is no “one size fits all” solution to information security. The security measures that are 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 individual's rights are comprised of:

- The right to be informed
    1. Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.
    2. You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with.
    3. You must provide privacy information to individuals at the time you collect their personal data from them.
    4. If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
    5. The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- The right of access
    1. Individuals have the right to access their personal data.
    2. This is commonly referred to as subject access.
    3. Individuals can make a subject access request verbally or in writing.
    4. You have one month to respond to a request.
    5. You cannot charge a fee to deal with a request in most circumstances.
- The right to rectification
    1. The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
    2. An individual can make a request for rectification verbally or in writing.
    3. QA have one calendar month to respond to a request.
    4. In certain circumstances QA can refuse a request for rectification.
    5. This right is closely linked to the controller's obligations under the accuracy principle of the GDPR (Article (5)(1)(d)).
- The right to erasure
    1. The GDPR introduces a right for individuals to have personal data erased.
    2. The right to erasure is also known as 'the right to be forgotten'.
    3. Individuals can make a request for erasure verbally or in writing.
    4. QA have one month to respond to a request.
    5. The right is not absolute and only applies in certain circumstances.
    6. This right is not the only way in which the GDPR places an obligation on you to consider whether to delete personal data.

- The right to restrict processing
    1. Individuals have the right to request the restriction or suppression of their personal data.
    2. This is not an absolute right and only applies in certain circumstances.
    3. When processing is restricted, you are permitted to store the personal data, but not use it.
    4. An individual can make a request for restriction verbally or in writing.
    5. You have one calendar month to respond to a request.
    6. This right has close links to the right to rectification (Article 16) and the right to object (Article 21).
- The right to data portability
    1. The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
    2. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
    3. Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
    4. The right only applies to information an individual has provided to QA.
- The right to object
    1. The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.
    2. Individuals have an absolute right to stop their data being used for direct marketing.
    3. In other cases where the right to object applies you may be able to continue processing if you can show that QA have a compelling reason for doing so.
    4. You must tell individuals about their right to object.
    5. An individual can make an objection verbally or in writing.
    6. QA have one calendar month to respond to an objection.

- 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. based on the individual's explicit consent.
    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 QA's 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;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Any suspected, reported or confirmed breach is logged with the IT Service desk, (0113 382 6200 or ITServiceDesk:@qa.com) who will manage the incident. The reporting person will be given a ticket number so progress and updates can be tracked.

3.2 Confirmation and Containment

The first step following a reported breach is to confirm the event and understand the asset impact – which may be data or other item compromise - as well as the set of circumstances that allowed the breach to happen. The root cause may be a process that requires revision or a technical element that requires modification.

Where the incident cannot be fully resolved immediately, the means by which the breach occurred will be isolated – thus if technical, the failing element should be disabled so that no further breaches can occur, and if a caused by a process, that process must be immediately ceased.

Once the breach is contained, the element leading to the breach will be analysed and enhanced to prevent future breaches. This will often involve input from specialists across the business such as IT, HR and Legal and in some cases contact with external stakeholders, suppliers, ICO and the Police.

3.3 Assessment of on-going Risk

Once the incident is contained, we must assess the risk and consequence of the breach.

The breach will be analysed so that QA understand the type of data involved and the points below assessed:

- What type of data is involved?
- How sensitive is the data (may be financial, personal or general)?
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?

Regardless of what happened to the data, it is important that the contents are understood so that overall risk is quantified. For example, sensitive data could mean very little to an opportunistic laptop thief whereas the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.

The scope of the breach is also quantified so that QA understand the extent of the risk – for example, is the data limited to one person or a number of people?

The assessment also considers the possible harm that could come to those individuals as a result of the breach. This is especially important if the breach puts at risk physical safety or reputation, or financial loss or a combination of these or other aspects of their life.

3.4 Notification of Breach

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. You must do this within 72 hours of becoming aware of the breach, where feasible.

When a personal data breach has occurred, QA need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then QA must notify the ICO; if it's unlikely then QA does not have to report it. However, if QA decide we don't need to report the breach, we need to be able to justify this decision.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals.

Recital 85 of the GDPR explains that:

"A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

When considering notification of the breach to the ICO and affected users, QA will consider the following:

- Will the breach result in a risk to people's rights and freedoms?
- Are there any legal or contractual requirements?
- Can notification help the individual, such as requesting the user makes password changes?
- If a large number of people are affected, or there are very serious consequences, we must inform the ICO.
- Consider how notification can be appropriately made as the extent of the breach must be put in context of the risk.

As a minimum, the communication to the affected users will include a description of how and when the breach occurred and what data was involved. QA will also include details of what has already been done to respond to the risks posed by the breach. Any suggested steps that the user can take to further protect themselves following the breach will also be communicated.

When QA reports a breach to the ICO, the GDPR mandates that we must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

The ICO recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So Article 34(4) allows you to provide the required information in phases, as long as this is done without undue further delay.

However, the ICO expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify the ICO of the breach when you become aware of it, and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to the ICO and tell them when you expect to submit more information.

The location for reporting breaches to the ICO is at https://ico.org.uk/for-organisations/report-a-breach/

It is also important to consider data surrounding the breach, and where the data incident involves data of a parent organisation (for example, a delegate's employer) we need to review the contract and where required, notify the customer's organisation. This is required under GDPR where QA are a data processor and the customer has remained as the data controller.

The contact points will vary within each organisation – so early communication with the QA Bids team to ascertain what contractual contact points are defined and also confirm who is the Account manager for that customer within QA.

The task for communication to the customer will be confirmed on a case by case basis, but is likely to be the responsibility of the Account manager along with the incident manager.

3.5 Evaluation and response

Once the breach has been fully understood and contained, it is important not only to investigate the causes of the breach but also to evaluate the effectiveness of our response to it.

If the breach was caused, even in part, by systemic and on-going problems, then simply containing the breach and continuing 'business as usual' is not acceptable; similarly, if our response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines responsibility in the light of experience.

The following points will be considered within the review process:

- Make sure QA fully understand how the personal data is acquired, processed, and where and how it is stored. This covers manual processes as well as within electronic systems.
- Establish where the biggest risks lie. For example, how much sensitive personal data do QA hold? Do we store data across the business or is it concentrated in one location?
- Risks will arise when sharing with or disclosing to others – both within QA, partners and customers. We must ensure that not only the method of transmission is secure but also that you only share or disclose the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced.
- Identify weak points in our existing security measures such as the use of portable storage devices or access to public networks.
- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice.

3.6 Liability

Clearly, any breach can result is liabilities surrounding the incident. The ultimate liability depends on whether QA are the data controller or data processor. However, if QA are the cause of the incident, then QA will be liable to some extent.

The law confirms that companies or their employees or representatives may be personally liable – confirmed within the GDPR and Employment Practices Code.

Everyone must remain mindful at all times that if they are the cause of a breach, they may be ***personally responsible*** for any fines that are imposed by the authorities.

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 includes 'any expression of opinion about the individual and any indication of the intentions of the Data Controller … in respect of the individual'. The definition is therefore quite broad, and may cover information such as an individual's health, beliefs, personal 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 by individuals who want to see a copy of the information an organisation holds about them. However, the right of access goes further than this, and an individual who makes a written request and pays a fee is entitled to be:

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and given details of the source of the data (where this is available).

In most cases you must respond to a subject access request promptly and in any event within one calendar month of receiving it.

Please refer to the QA SAR Policy Guidance document which can be found on the G drive.