

QG-GDPR Questionnaire B.

Requirements for a GDPR Management System

Introduction

Completion of this questionnaire and its subsequent approval by a QG Accredited Certification Body will verify that the submission meets the QG-GDPR Fundamentals level of assurance against the QG-GDPR Management Standard.

The main objective of the QG-GDPR Fundamentals assessment is to determine that your organisation has effectively implemented the requirements of the QG-GDPR Management Standard, in order to minimise inconsistency of your supply or service.

The completed questionnaire attests that you meet the requirements of GDPR Fundamentals, which must be approved by a Board member or equivalent, and will then be verified by a competent assessor from a **certification body**. Such verification may take a number of forms, and could include, for example, a telephone conference. The verification process will be at the discretion of **QG Business Solutions**.

Scope of GDPR Fundamentals

The Scope is defined as the areas that will have an effect on your customer relationship. This scope will be printed on your certificate of compliance.

You will be required to identify the actual scope of the system to be evaluated as part of the questionnaire. **You have chosen this questionnaire because you**

Employ less than 250 who process personal data that could result in a risk to the rights and freedoms of individuals, special categories of personal data OR criminal convictions and offences.

How to avoid delays & additional charges

You may incur additional charges if details are not sufficiently supplied, answer the questions as fully as possible giving supporting comments, paragraphs from policies and screen shots where possible.

As a rule of thumb if it takes longer to assess the submission than you spent preparing it, you may be charged.

Organisation Identification

Please provide details as follows:

Organisation Name (legal entity):	
Sector:	
Parent Organisation name (if any):	
Size of organisation micro, small, medium, large. (See definition below)	
No of employees	
Point of Contact name: Salutation (Mr, Mrs, Miss etc) Initial First Surname	
Job Title:	
Email address:	
Telephone Number:	
Main web address for company in scope:	
Building Name/Number Address 1 Address 2 Address 3 City County Postcode	

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

Certification Body:	
Do you wish to be included in the register of QG Management Standards certified companies. Exclusion means customers will not be able to find your entry. If this is left blank you will be excluded.	
From time to time QG Business Solutions and other interested bodies may wish to use your company for marketing QG Essentials programmes. If you wish to be promoted in this way please enter YES in the box. If this is left blank it is deemed your consent is NOT given.	

SME Definition

Company category	Employees	Turnover	or	Balance sheet total
Medium-sized	< 250	≤ € 50 m		≤ € 43 m
Small	< 50	≤ € 10 m		≤ € 10 m
Micro	< 10	≤ € 2 m		≤ € 2 m

Business Scope

For the purposes of GDPR Essentials the scope should include all those parts of the business that affects your customer/suppliers and partners. You are not required to answer questions that are greyed out

Please identify the scope of the system to be assessed under this questionnaire, including locations.

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

Conformance Statement

We employ less than 250 who process personal data that could result in a risk to the rights and freedoms of individuals, special categories of personal data OR criminal convictions and offences..

Please continue to state your company scope

1. Data Protection Policy

Objective

To publicly declare the data protection values of the company.

	Requirement	Evidence/Narrative
1.	Is there a written data protection policy in place and does it define ;	
1.1	management commitment including responsibility of different levels of management and individuals?	

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

1.2	definitions of personal data, special categories of personal data, processing, filing systems, controller, processor, consent, data subject and personal data breach?	
1.3	legal rights of data subject on processing personal data including children aged under 16 and aged 16 or over?	
1.4	legal principles relating to processing of personal data including transparency	
1.5	that making a request for personal data is free unless a reasonable cost is to be charged where requests are unfounded or excessive or repetitive in character	
1.6	Data subject access requests to be acted upon within 1 month	
1.7	how an individual can request access to their personal data	
1.8	how personal data will be deleted	
1.9	how and what personal data will be provided in response to a request	
1.10	when data will be provided in a commonly used electronic format	
1.11	how to complain	
1.12	Is the policy dated	
1.13	Has it been reviewed in the last 12 months.	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

Data Protection Policy

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

2. Management Responsibilities

Objective

To ensure the organisations management understand their responsibilities for Data Protection.

	Requirement	Evidence/Narrative
2	Are management responsibilities defined in writing?	
2.1	Do managers know what their responsibilities are?	
2.2	Has the organisation established if it requires a Data Protection Officer?	
2.2.1	If so, has their name/role been documented?	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Signed training register / roles responsibility description stating section responsibility

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

3. Data Protection Objectives

Objective

To ensure the organisation is able to deal with Data Protection legislation in a consistent manner.

	Requirement	Evidence/Narrative
3.1	Are the company data protection objectives stated in writing?	
3.2	Is the scope defined?	
3.3	Is there a list of definitions?	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Document register with an expected review date and actual review date (signed)

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

4. Obtaining Consent

Objective

To ensure that consent is obtained prior to processing

	Requirement	Evidence/Narrative
4.1	Has a written declaration been produced for 'consent to processing'?	
4.2	How are data subjects asked to opt in?	
4.3	Are pre-ticked boxes or any other consent by default utilised?	
4.4	Has the organisation been through a checking process to ensure data subject facing documentation is clear and uses plain language?	
4.5	What statement is offered to data subjects to revoke their consent?	
4.6	What are the timeframes set for withdrawal of consent in the organisations process ?	
4.7	Are products or services in marketing literature offered in other languages?	
4.7.1	Do consent processes mirror these languages?	
4.8	What messages are used to explain how the data subjects personal data will be used?	
4.8.1	Is the organisation and any third party identified in the documentation?	
4.9	Is a process in place to assess that consent is freely given?	
4.10	Is a process in place to verify the age of a data subject when it's a minor?	

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

4.11	Is a record kept of when and how consent was obtained and what the data subject was told at the time?	
4.12	Is there a process in place to review consents?	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Records of how and when consent was obtained and what the data subject was told at the time.

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

5. Collection of Personal Data

Objective

To ensure personal data is only collected and processed in compliance with data protection legislation.

	Requirement	Evidence/Narrative
5.1	Has the organisation reviewed, in the last 12 months, what personal data it holds, the source of personal data held and who it is shared with?	
5.2	Has the organisation categorised personal data and identified special categories of personal data held?	
5.3	Has the organisation reviewed, in the last 12 months, how consent was obtained, reviewed consents given and renewed consent if required?	
5.4	Where data is collected direct from the data subject, are they provided, at the time of collection, with an information notice in a concise, transparent intelligible and easily accessible manner (whether in writing or by other means including electronic) setting out the required legal information*?	
5.5	Where the data has not been collected direct by the organisation from the data subject, has the organisation provided an information notice to the data subject? (at the latest within one month of having obtained the personal data if section 5.6 is not satisfied)	

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

5.6	Are checks carried out and written confirmation obtained from the third party to ensure that where personal data has not been obtained direct by the organisation from the data subject?	
5.7	Has the organisation assigned responsibility to third party organisations who may collect data on your behalf on provision of information notices, review of notices, updating notices and consent ?	
5.8	Has the organisation assessed which departments/ areas will be impacted by the new requirements for issuing information notices?	

*Required legal information

- The identity and contact details for the organisation
- The contact details of the data protection officer (if applicable)
- The purposes of the processing as well as the legal basis for the processing using clear and plain language
- If a public authority, the legitimate interests if relied on
- The recipients or categories of recipients of the personal data
- Whether the organisation intends to transfer the data to a third country or international organisation and what appropriate and suitable safeguards there are or whether there is an adequacy decision for such transfer
- The retention period of the data or the criteria that is used to determine this
- The right to request access to, rectification of, erasure of personal data and the restriction of or object to processing
- The right to request data portability
- The right to withdraw consent at any time
- The right to make a complaint to the supervisory authority
- If the personal data is required by law or contract or is a necessary requirement to enter into a contract and the possible consequences of failure to provide such data

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

- Whether automated decision making is to take place including profiling and meaningful information on the logic to be used and the envisaged consequences of such automated decision making

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Information asset register containing information source and who it is shared with complete with expected review date and actual review date (signed).
Review records of how consent is given (expected date and actual date)

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

6. Processing Personal Data

Objective

To ensure that personal data is only processed for the purposes for which it was given

	Requirement	Evidence/Narrative
6.1	Is there a written record of processing for the activities under the responsibility of each data controller or representative of the controller? (This includes electronic form.)**	
6.1.1	Do you use data processors? If NO go to 6.2	
6.1.2	Do the data processors maintain a written record of all processing activities carried out of your behalf? ***	
6.2	Does the organisation undertaken data protection impact assessments (DPIA) on any high risk processing activity before commencement?	
6.2.1	If so is evidence available that you sort the views of the affected data subjects or their representatives.	
6.2.2	Do you have evidence that you consulted with the supervisory authority when your DPIA identified a high level of unmitigated risk?	
6.3	Does the organisation assess whether any new processing purpose is compatible with the purpose for which the data was initially collected?	

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

6.4	Is a new information notice provided to the data subject on any further processing not covered by an original information notice prior to commencing such processing?	
6.5	Is there a process in place to regularly review and randomly audit that any processing is being undertaken in compliance with the purposes for which the personal data was given?	
6.6	Is there a process in place to undertake regular checks that the personal data being processed is relevant and limited to what is necessary only for the purpose for which it was given?	
6.7	Have you obtained verification, in writing, that the personal data being given is accurate at the time it is collected or received and is still accurate?	
6.8	Is an annual review process in place to keep personal data up to date which includes reviews of the data, requesting that the data subject checks the data provided remains accurate with any amended data. ?	
6.8.1	Is there a process under which the data subject can inform you of any inaccurate data at any time?	
6.9	Is there a process in place to ensure Inaccurate data is erased securely or corrected without delay?	
6.9.1	Is there a process in place to ensure that any requests for rectification is dealt with without undue delay?	
6.9.2	Is there a process in place to complete any incomplete personal data?	

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

6.10	Do you regularly weed personal data held to ensure that it is not held for longer than is necessary in compliance with the retention periods set out in any information notices provided to the data subjects?	
------	--	--

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Results of Data Protection Impact Assessments
Records of random compliance audits (checking the data being used as expected)
Written verification that data being used is accurate at the time of collection Records of any data that were erased or corrected due to an initial error (including date and time and who changed it and why)

**** Required Written Record (Applicant)**

Records are required to contain the following information

- the name and contact details of the controller, any joint controller, the controller's representative and data protection officer if there is one
- the purposes of the processing
- a description of the categories of data subjects and the categories of personal data
- categories of recipients to whom the data has been or will be disclosed
- any transfers to a third country including the name of the third country or international organisation and details of any safeguards if appropriate
- time limits for the erasure of the different categories of data
- a general description of the technical and organisational security measures
- instructions to enable records to be made available to the supervisory authority on request.

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

*** Required Written Record (data processors)

- the name and contact details of the processor and the controller for whom the processor acts and their representatives and, if applicable, the data protection officer
- the categories of processing carried out for each controller
- transfers to any third countries or international organisation and their details and if appropriate details of suitable safeguards
- a general description of the technical and organisational security measures being used
- instructions to enable records to be made available to the supervisory authority on request.

7. Safeguarding Personal Data

Objective

To ensure that personal data is only processed in a manner that it ensures appropriate security against unauthorised or unlawful processing.

	Requirement	Evidence/Narrative
--	-------------	--------------------

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

7.1	Having regard to the state of art, cost of implementation and the nature, scope, context and purposes of processing and the risks to the rights and freedoms of the data subjects, do you implement appropriate technical and organisational measures such as encryption, pseudonymisation or data minimisation in an effective manner and integrate necessary safeguards into the processing to render data unintelligible in case of unauthorised access?	
7.2	Do you regularly test, assess and evaluate the effectiveness of technical and organisational measures for ensuring security?	
7.2.1	Do you update technical and organisational measures for ensuring security where necessary?	
7.3	Is there a process in place to ensure only staff required to undertake the processing or monitoring or auditing have access to personal data?	
7.3.1	Are controls in place to ensure that staff only undertake processing on instructions from the organisation?	
7.4	Are regular checks carried out to ensure compliance with the requirement to use the appropriate measures?	
7.5	Is there a process in place to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services?	
7.6	Are controls in place to be able to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident?	

7.7	Is there an internal breach notification procedure in place ensuring that breaches are notified without undue delay?	
7.7.1	In circumstances where the supervisory authority requires informed does the procedure include not later than 72 hours after becoming aware of the breach?	
7.8	Does the organisation regularly test and review the internal breach notification procedure?	
7.9	Has an internal breach register been implemented and maintained?	
7.10	Do you have a process for when breaches occur that you identify the incident and reasons for it, its effects, and any patterns of behaviour and identify and implement a response plan/ remedial action to ensure non-repetition?	
7.11	When using data processors do you ensure that all arrangements are in signed contractual form and detail the elements mentioned in the Regulation and the obligations on the processor to comply with the Regulation?	
7.11.1	Do you only use processors that provide sufficient written guarantees on the use of appropriate technical and organisational measures to ensure protection of the rights of the data subject?	
7.11.2	Do you have a process in place to ensure processors cannot engage another processor without the prior written consent of the organisation and cannot transfer personal data to a third country or an international organisation without the written instructions of the organisation?	

7.11.3	Does your Processor documentation include that all staff undertaking the processing for the processor have signed up to confidentiality?	
7.11.4	Does your process ensure that all processors return or delete securely any personal data including copies as required by the organisation in particular at the end of the provision of the services?	
7.12	Is a process in place that defines when destroying personal data whether in manual form or electronic ensure that the destruction is undertaken securely, confidentially and permanently?	
7.12.1	When using contractors to undertake this task (7.12) has a signed written contract been agreed ensuring their obligations to comply with data protection legislation?	
7.13	When introducing new technology is there a process in place to ensure privacy by design is built in?	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Risk assessment register (with relevant technical controls to mitigate risks to acceptable levels)
Results of technical health checks (Cyber Essentials Plus reports etc)
Records of random checks to ensure technical controls are working.
Record of all Breaches that have been reported (including time lag, outcomes, remediation, lessons learned)
Records of business continuity tests
Records of removal / return /destruction of Data assets. And signed contract of third parties used in data destruction.

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

Letters of assurance from vendors saying they have privacy built in by design.

8. Dealing with Requests for Access by Data Subjects

Objective

To ensure that access requests from data subjects are dealt with correctly and within their legal rights.

	Requirement	Evidence/Narrative
8.1	Has the organisation implemented and publically published a procedure for dealing with any data subject access requests?	
8.1.1	Does the procedure detail that requests are dealt with without undue delay and at the latest within one month and a nominated person or team is identified to co-ordinate the gathering of the data requested?	
8.1.2	Does the procedure identify the name of the contact to whom such requests should be sent and where they should be sent to?	
8.1.3	Does the procedure include a complaints stage for any data subjects unsatisfied with the original decision, which also refers to the next stage of being able to make a complaint to the supervisory authority?	
8.1.4	Does the procedure include that if the request is unclear or the organisation holds a large quantity of data that could satisfy the request requirements, a process to clarify the information requested or the processing activities to which the request relates?	
8.1.5	Does the procedure consider applicable exemptions before providing the data requested and whether redacting the data is appropriate or whether another's consent is required before disclosure if the data requested contains another's personal data?	

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

8.2	Have template letters been issued to be used in response to a request?	
8.3	Has evidence of 8.1 been documented	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Training record that staff understand Subject Access Requests.
Subject Access Request register
Register of complaints in regards to Subject Access Requests.
Access Request Procedure
Exemptions and further consent register

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

9. Dealing with Requests for Data Portability

Objective

To ensure that for data portability requests from data subjects are dealt with within their legal rights.

	Requirement	Evidence/Narrative
9.1	Is a process established to receive and provide data in a commonly used electronic form?	
9.2	Is the organisation capable of providing information in a structured, commonly used and machine readable form?	
9.3	Is the organisation capable of transmitting personal data directly to another organisation without hindrance?	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Subject Access Request register

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

10. Data Subject Right to Object or Restrict Processing

Objective

To ensure that processing any communications whereby the data subject objects to processing for direct marketing or wishes to restrict processing ???????

	Requirement	Evidence/Narrative
10.1	Are employees, including those responsible for sales and marketing, informing data subjects of their right to object to direct marketing clearly and separately from other information?	
10.2	A process is in place to ensure if a data subject objects to direct marketing, the data is not be used for direct marketing any further?	
10.3	Are automated systems activated for data subjects to object to the direct marketing eg unsubscribe to emails?	
10.4	Is a process in place to manage a request to restrict processing on the basis that the data accuracy is disputed or the individual has objected to the processing?	
10.4.1	Is a process in place where the organisation is checking the grounds for an objection or the processing is unlawful but the individual does not want the data erased or the organisation no longer needs the data but the individual requires the personal data to remain to establish, exercise or defend legal claims, the data will only be held and not processed until that restriction is lifted?	

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

10.4.2	Does the organisation have a system in place to notify the data subjects before lifting restriction in 10.	
10.4.3	Does the process described in 10.4.1 allow for such data that has been disclosed to others, notify the recipients of the restriction and latterly of any lifting of the restriction?	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Records of any Data subject that wishes processing to be restricted (such as for the purposes of direct mail).

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

11. Dealing with Requests for Erasure of Data (Right to be forgotten)

Objective

To ensure that the organisation correctly deals with request to have a data subject's personal data erased

	Requirement	Evidence/Narrative
11.1	Is a process in place to ensure that on receipt of a request to have personal data erased the organisation will erase such data without undue delay?	
11.1.1	Does the process identify erasure if the data is no longer necessary for the purpose for which it was collected or processed or if the data subject withdraws consent to the processing?	
11.2	Has the organisation implemented a system whereas it has made the personal data public, to erase the data?	
11.2.1	Does this system include the process whereas the data has been disclosed to others that, where possible that data is erased?	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Record of all data requests for the right to be forgotten (erasing info)

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

12. Use of Profiling and Automated Decision Making

Objective

To ensure that the organisation is legally compliant when automated decision making and profiling is used.

	Requirement	Evidence/Narrative
12.1	The organisation has a system in place to provide fair processing information about solely automated decision making including profiling which includes meaningful information about the logic involved such as the categories of data used to create a profile, the source of the data and why this data is relevant?	
12.2	Has a data protection impact assessment (DPIA) been carried out when systematic and extensive automated processing including profiling is required?	
12.2.1	Has the organisation undertaken regular reviews to assess if processing is performed in accordance with the DPIA?	
12.3	Does the organisation use appropriate mathematical or statistical procedures to safeguard individuals' rights and freedoms when carrying out automated processing or profiling?	
12.4	Has the organisation implemented a procedure whereby a data subject can request not to be subject to a decision based solely on automated processing?	

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

12.4.1	Does the process ensure that there is human intervention for the data subject to express his or her views too and contest the decision of the organisation?	
12.5	Has a system been put in place to ensure that the organisation does not use solely automated decision -making on the special categories of personal data as set out in the data protection legislation or in relation to a child	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Data Protection Impact Assessment results in regards to profiling

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

13. Transfer of Personal Data to Third Countries or International Organisations

Objective

To ensure that the transfer of personal data to third countries or international organisations are compliant with the legal requirements of the data protection legislation.

	Requirement	Evidence/Narrative
13.1	Does the organisation ensure there is an adequate level of protection defined by a national authority when transferring personal data to a third country or international organisation?	
13.2	Does the organisation has reviewed and will regularly review key international data flows to ensure compliance with the Regulation	
13.3	Does the organisation regularly review its contract arrangements with service providers and customers/clients/ organisations outside of the EEA?	
13.3.1	Where no adequacy decision has been made, has the organisation defined that personal data will only be transferred where the organisation or the contracted processor has provided appropriate safeguards, as defined by the Regulation, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available?	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

Document
Records of all data transferred to third countries and international origins

14. Training and Awareness

Objective

To ensure that staff whether directly or indirectly processing personal data have the skills and knowledge to process the data.

	Requirement	Evidence/Narrative
14.1	Are all staff trained both at induction and as annual training in in dealing with personal data?	
14.2	Has staff who process personal data had in-depth training in processing personal data?	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Security Awareness training register signed by individuals

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

15. Complaints

Objective

To ensure that complaints are dealt with in a timely manner

	Requirement	Evidence/Narrative
15.1	<p>Is a procedure in place that covers</p> <ul style="list-style-type: none">○ Who is responsible for handling the complaint○ What timescales are expected for responses○ How the complaint will be dealt with○ What is the escalation process	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
records of all complaints (and how dealt with and follow ups required)

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

16. Management Review

Objective

To ensure that this management system is being implemented effectively

	Requirement	Evidence/Narrative
16.1	Is a system in place that reviews <ul style="list-style-type: none">○ Policy○ Objectives○ Outputs○ Effectiveness	
16.2	Is there an annual review which is documented and acted upon?	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Minutes of management review

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

17. Audit

Objective

To ensure that the management system is in working to plan

	Requirement	Evidence/Narrative
17.1	Are random checks carried out to ensure compliance with the requirement to use the appropriate measures?	
17.2	Is an annual audit is in place that checks that information held is compliant?	
17.3	Is an audit process is in place that checks the system at least once per year?	

Your Certification Body is looking for evidence that you have met the requirements, any easy way to provide this is to attach a live version of the document listed below.

Document
Audit Report

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions

Approval

It is a requirement of the Scheme that a Board level (or equivalent) of the organisation has approved the information given. Please provide evidence of such approval:

When you have completed the document you should email it to;

Brian Lightowler

01228 631681

gdpr@qgbiz.co.uk

REMEMBER TO ENSURE IT HAS BEEN SIGNED BY A SENIOR MEMBER OF YOUR COMPANY.

Document No. QG0203 Updated 14/06/2018

Authorised BL Company QG Business Solutions