

GDPR Essentials

Requirements for a Managed System

Requirements for a Managed GDPR System

The General Data Protection Regulation – GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

QG Management Standards have devised a standard to assist organisations in the compliance of the new requirements. The QG GDPR Management Standard has been written using the principles of General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

This standard applies to all organisations who are 'controllers' **and/or** 'processors'. The definitions are broadly the same as under the Data Protection Act – ie the controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are currently subject to the Data Protection Act, it is likely that you will also be subject to the GDPR.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

The following requirements should be used to inform your questions whilst completing the QG GDPR questionnaire. If you are applying for GDPR PLUS your systems will be audited against these requirements.

QG Information GDPR Management Standard

No.	Section	Standard	Deliverables
1	Data Protection Policy	A written data protection policy is in place that sets out clearly the legal obligations under data protection legislation.	<p>The policy is in writing and includes as a minimum:</p> <ul style="list-style-type: none"> • management commitment including responsibility of different levels of management and individuals • definitions of personal data, special categories of personal data, processing, filing systems, controller, processor, consent, data subject and personal data breach • legal rights of data subject on processing personal data including children aged under 16 and aged 16 or over • the legal principles relating to processing of personal data*1 • 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 • Complying with data subject access requests within 1 month • how an individual can request access to their personal data • how personal data will be deleted • how and what personal data will be provided in response to a request • when data will be provided in a commonly used electronic format • how to complain • dated • minimum annual review
			<p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • Signed Policy Document
2	Management Responsibilities	Management responsibilities are defined in writing	<p>Organisation ownership is defined, in writing and by section</p> <ul style="list-style-type: none"> • Evidence is in place that individuals understand that they have section responsibility

			<ul style="list-style-type: none"> To identify if required and appoint a trained data protection officer to help demonstrate compliance. To nominate a person or team to co-ordinate the gathering of any data requested
			<p>Documents (evidence) Required</p> <ul style="list-style-type: none"> Signed training register / roles responsibility description stating section responsibility.
3	Data Protection Objectives	Company data protection objectives are documented, agreed and reviewed	<p>A written system is in place that details;</p> <ul style="list-style-type: none"> objectives, scope definitions <p>A system is in place that reviews and updates objectives on a regular basis (minimum yearly)</p>
			<p>Documents (evidence) Required</p> <ul style="list-style-type: none"> Document register with a expected review date and actual review date (signed)
4	Obtaining Consent	Unambiguous, specific, informed, freely given consent must be obtained prior to processing unless another condition in the Regulation is satisfied.	<ul style="list-style-type: none"> Consent to processing is contained in a written declaration produced by the organisation and must be distinguishable from other matters in that declaration and is clearly distinguishable in any longer document by being prominent Data subjects are asked to positively opt in The organisation does not use pre-ticked boxes or any other type of consent by default Use of clear and plain language Data subject is informed of right to revoke their consent at any time Revocation of consent is as easy to do as giving consent and is acted upon without undue delay Does the consent need to be in a number of different languages The purpose(s) for which the personal data is to be used is/are distinct and legitimate and explained in clear, easily understood and transparent terms. The organisation is named and any third parties to whom the data is to be disclosed are identified When assessing if consent is freely given, utmost account is taken of whether the performance of a contract including provision of a service is conditional on consent to

			<p>processing personal data which is not necessary for the performance of that contract</p> <ul style="list-style-type: none"> • The organisation can identify and verify the age of the data subject and seek parental consent where required • The organisation keeps a record of when and how the consent was obtained and what the data subject was told at the time • The organisation regularly reviews consents given to check that the data, processing and purposes have not changed and renewed consents are requested when required
			<p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • Records of how and when consent was obtained and what the data subject was told at the time.
5	Collection of Personal Data	Personal data is only collected and processed in compliance with data protection legislation	<ul style="list-style-type: none"> • The organisation has reviewed in the last 12 months what personal data it holds, the source of personal data held and who it is shared with and will regularly review this by way of an information audit • The organisation categorises personal data and identifies special categories of personal data held • The organisation has reviewed in the last 12 months how consent was obtained and regularly reviews consents given and renews consent if required • Where consent is required, Standard 4 is followed • If the data is collected direct from the data subject, the data subject is 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 being <ul style="list-style-type: none"> ○ 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

			<p>international organisation and what appropriate and suitable safeguards there are or whether there is an adequacy decision for such transfer</p> <ul style="list-style-type: none"> ○ 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 ○ 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 <ul style="list-style-type: none"> ● If the data has not been collected direct by the organisation from the data subject, the organisation will provide an information notice to the data subject, if the data subject has not already received this information, at the latest within one month of the receipt of the data or at the time of the first communication with the data subject if the personal data is to be used to communicate with the data subject or if the data is to be disclosed to another recipient than at the latest when that personal data is disclosed to the other recipient. ● Checks are carried out and written confirmation is obtained from the third party to ensure that where personal data has not been obtained direct by the organisation from the data subject, wherever possible the data subject has already received the relevant legally required information set out in an information notice (see above) ● Assign responsibility with third party organisations who may collect data on your behalf on provision of information notices, review of notices, updating notices and consent ● The organisation has assessed which departments/ areas will be impacted by the new requirements for issuing information notices <p>Documents (evidence) Required</p> <ul style="list-style-type: none"> ● Information asset register containing information source and who it is shared with
--	--	--	--

			<p>complete with expected review date and actual review date (signed).</p> <ul style="list-style-type: none"> Review records of how consent is given (expected date and actual date)
6	Processing Personal Data	Personal data is only processed for the purposes for which it was given and in compliance with the Regulation	<ul style="list-style-type: none"> If the organisation employs 250 employees or more or processes special categories of personal data, keep additional required records of the organisation's high risk processing activities which are compliant with the requirements of the Regulation Undertake data protection impact assessments (DPIA) on any high risk processing activity before it is commenced. Seek the views of the affected data subjects or their representatives when conducting a DPIA. Consult with the supervisory authority if the DPIA identifies a high level of unmitigated risk. Assess whether any new processing purpose is compatible with the purpose for which the data was initially collected Provide a new information notice to the data subject on any further processing not covered by an original information notice prior to commencing such processing Regularly review and randomly audit that any processing is being undertaken in compliance with the purposes for which the personal data was given. 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 Get verification in writing that the personal data being given is accurate at the time it is collected direct or has been received and is still accurate. Keep personal data up to date by undertaking regular reviews of the data and requesting that the data subject checks the data provided for accuracy and provides you with any amended data. Have a process whereby this is undertaken at least annually but also have a process under which the data subject can inform you of any inaccurate data at any time. Inaccurate data must be erased securely or corrected without delay and any requests for rectification must be dealt with without undue delay. The data subject may require the organisation to complete any incomplete personal data. 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

			<p>data subjects.</p> <p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • 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)
7	Safeguarding Personal Data	<p>Personal data is only processed in a manner that ensures appropriate security of the data including protection against unauthorised or unlawful processing and against accidental or unlawful loss, destruction, alteration, unauthorised disclosure of or access to personal data or damage using appropriate technical or organisational measures which may include encryption or pseudonymisation</p>	<ul style="list-style-type: none"> • 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, 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 • Regularly test, assess and evaluate the effectiveness of technical and organisational measures for ensuring security and update them where necessary • Only staff required to undertake the processing or monitoring or auditing have access to the personal data and only undertake processing on instructions from the organisation • Random checks are carried out to ensure compliance with the requirement to use the appropriate measures • Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services • Be able to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident • Have an internal breach notification procedure ensuring that breaches are notified without undue delay.

			<ul style="list-style-type: none"> • Ensure that the procedure requires breaches to be reported where required without undue delay to the supervisory authority and where feasible not later than 72 hours after becoming aware of it • Regularly test and review that internal breach notification procedure is effective • Maintain an internal breach register • When breaches occur identify the incident and reasons for it, its effects, any patterns of behaviour and identify and implement a response plan/ remedial action to ensure non-repetition • When using data processors 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. 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. • 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 • Ensure all staff undertaking the processing for the processor have signed up to confidentiality • Ensure 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 • Where destroying personal data whether in manual form or electronic ensure that the destruction is undertaken securely and confidentially and permanently. • Ensure any contractors used to undertake this task have a signed written contract ensuring their obligations to comply with data protection legislation*2 • All new technology has privacy by design built in <p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • Risk assessment register (with relevant technical controls to mitigate risks to acceptable levels)
--	--	--	--

			<ul style="list-style-type: none"> • Results of technical health checks (Cyber Essentials Plus reports etc) • Records of random checks to ensure technical controls are working. • Record of regular backups and restore operations to test backup is 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. • Letters of assurance from vendors saying they have privacy built in by design.
8	Dealing with Requests for Access by Data Subjects	Deal with any requests for access by data subjects correctly within their legal rights	<ul style="list-style-type: none"> • Have a known set procedure for dealing with any data subject access requests without undue delay and at the latest within the set legal deadline of one month and a nominated person or team to co-ordinate the gathering of the data requested • Publish the name of the contact to whom such requests should be sent and where they should be sent to simplify the process • Make sure public facing staff have been trained and can identify an access request and know where to refer it without delay • Make sure staff know how to verify the identity of the data subject making the request • If the request is unclear or the organisation holds a large quantity of data that could satisfy the request requirements then request clarification as to information requested or the processing activities to which the request relates • Develop template letters in response to a request to ensure acknowledgement of the request and to ensure all elements of supporting information are provided in the final response. • 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 • Have an internal complaints stage for any data subjects unsatisfied with the original

			<p>decision which also refers to the next stage of being able to make a complaint to the supervisory authority</p> <ul style="list-style-type: none"> • Keep an internal record of data subject access requests received
			<p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • Training record that staff understand Subject Access Requests. • Subject Access Request register (including format of the information requested – in respect to standard 9) • Register of complaints in regards to Subject Access Requests. • Access Request Procedure • Exemptions and further consent register
9	Dealing with Requests for Data Portability	Deal with any requests from a data subject for data portability within the legal rights of the data subject	<ul style="list-style-type: none"> • If a request is received for access to the personal data of a data subject in a commonly used electronic form then the organisation should provide the data in a commonly used electronic form unless the data subject requests otherwise • The organisation can be required to provide information in a structured, commonly used and machine readable form and must comply with this request, subject to any applicable exemptions, where the personal data is being processed by electronic means, was provided to the organisation by the data subject and where the legal basis for processing is consent from the data subject or to fulfil a contract or steps preparatory to a contract being entered into • A data subject can also request that their personal data is transmitted directly to another organisation without hindrance by the organisation where it is technically feasible to do so.
			<p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • (see 8.2)

10	Data Subject Right to Object or Restrict Processing	Processing any communications from a data subject whereby the data subject objects to processing for direct marketing or wishes to restrict processing in compliance with their rights under the Regulation	<ul style="list-style-type: none"> • The data subject is told of their right to object to direct marketing clearly and separately from other information at the latest at the time of the first communication • If a data subject objects to direct marketing, the data is not be used for direct marketing any further as this is an absolute right of the data subject • If it is an online service the data subject is able to object to the direct marketing by automated means too eg unsubscribe to emails • If a request to restrict processing is received from a data subject on the basis that the data of the accuracy is disputed or the individual has objected to the processing and the organisation is checking the grounds for such 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 either by the organisation or by the individual depending on the grounds for the restriction. The organisation will notify the individual before lifting a restriction. • If such data has been disclosed to others, the organisation will notify the recipients of the restriction and latterly of any lifting of the restriction. <p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • Records of any Data subject that wishes processing to be restricted (such as for the purposes of direct mail).
11	Dealing with Requests for Erasure of Data (Right to be forgotten)	In compliance with data protection legislation correctly dealing with request to have a data subject's personal data erased.	<ul style="list-style-type: none"> • On receipt of a request from a data subject to have personal data erased the organisation will erase such data without undue delay, unless an exemption set out in the legislation exists such as right of freedom of expression and information or archiving purposes in the public interest, 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 and there is no other legal basis for the processing or the personal data has been unlawfully processed or erasure is required to comply with a national legal obligation

			<ul style="list-style-type: none"> • If the organisation has made the personal data public and is obliged to erase the data, taking into account available technology and the cost of implementation, the organisation will take reasonable steps, including using technical measures itself, to inform other organisations which are processing the data that the data subject has requested erasure by such organisations of any links to or copies of or replication of that personal data • If the organisation has disclosed the personal data to be erased to others, the organisation will notify those others, where possible, of the requirement to erase that data
			<p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • Record of all data requests for the right to be forgotten (erasing info)
12	Use of Profiling and Automated Decision Making	Legally compliant use of automated individual decision-making including profiling and dealing with any requests not to be subject to such from a data subject within their legal rights	<ul style="list-style-type: none"> • The organisation provides 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 • The organisation undertakes a data protection impact assessment (DPIA) when systematic and extensive automated processing including profiling is required • The organisation will undertake necessary regular reviews to assess if processing is performed in accordance with the DPIA • The organisation uses appropriate mathematical or statistical procedures to safeguard individuals' rights and freedoms when carrying out automated processing or profiling • A data subject can request not to be subject to a decision based solely on automated processing including profiling which produces legal or similar effects concerning him or her. If such a request is received it will be complied with unless the decision is necessary for the entering into or performance of a contract, is authorised by national law with suitable safeguards or is based on the explicit consent of the data subject • If such a request is received the organisation will ensure that there is human intervention for the data subject to express his or her views too and contest the decision of the organisation. • The organisation will 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
			<p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • Data Protection Impact Assessment results in regards to profiling
13	Transfer of Personal Data to Third Countries or International Organisations	All transfers of personal data to third countries or international organisations are compliant with the legal requirements of the data protection legislation	<ul style="list-style-type: none"> • The organisation will transfer personal data to a third country or international organisation where the relevant national authority has decided that there is an adequate level of protection. • The organisation has reviewed and will regularly review key international data flows to ensure compliance with the Regulation • The organisation has reviewed its contract arrangements with service providers and customers/clients/organisations outside of the EEA and if no adequacy decision has been made, 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
			<p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • Records of all data transferred to third countries and international origins
14	Training & Awareness	All staff are trained at induction and regularly thereafter (minimum once a year) on data protection to help demonstrate compliance.	<p>Training is undertaken for all staff both at induction and as annual training and includes:</p> <ul style="list-style-type: none"> • The principles relating to data protection • What is personal data • Know scams • How to report a potential breach • The requirement to use and use of appropriate security, technical and organisational

			<p>measures (see section 7)</p> <ul style="list-style-type: none"> • Internal breach notification procedure • How to identify an access request and who to refer to <p>Staff who process personal data are required to also undertake training in the following areas;</p> <ul style="list-style-type: none"> • the legal principles relating to processing • legal rights of data subjects • how data is collected • how to obtain unambiguous, specific, informed, freely given consent in a lawful, fair and transparent manner • how to explain the specified, explicit and legitimate purpose(s) for processing • how to ensure data is adequate, relevant, limited, accurate and up to date • what to do if a data subject requests that their personal data is erased or rectified or wishes to withdraw consent or objects to the processing • auditing data • how to protect the security of the data and what measures must be used to do so • where and how data is kept • how to deal with a data subject request • how to verify the identity of the data subject • how to deal with a request to port the data subject's data to a new organisation • when and how to anonymise data (pseudonymisation) • how to report a personal data breach • how to verify the identity of the data subject making an access request <p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • Security Awareness training register signed by individuals
--	--	--	---

15	Complaints	A system is in place to deal with complaints	<ul style="list-style-type: none"> • A procedure is in place that identifies <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 <p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • records of all complaints (and how dealt with and follow ups required)
16	Management Review	A system is in place to review the effectiveness of the GDPRMS	<p>A system that reviews</p> <ul style="list-style-type: none"> ○ Policy ○ Objectives <p>On an annual basis is documented and acted upon</p> <p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • Minutes of management review
17	Audit	An internal and/or third part audit is carried out at regular intervals.	<ul style="list-style-type: none"> • Random checks are carried out to ensure compliance with the requirement to use the appropriate measures • An annual audit is in place that checks that information held is compliant • An audit process is in place that checks the system at least once per year. <p>Documents (evidence) Required</p> <ul style="list-style-type: none"> • Audit results.

Additional Requirements

Requirement	Standard	Deliverables
Data Protection Officers must be appointed for all	To identify if required and appoint a trained data protection	<ul style="list-style-type: none"> • train the data protection officer either internally or externally or both in all the legal requirements of the data protection legislation

<p>public authorities or bodies or other organisations (non public sector) where the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities.</p> <p>And in all cases the core activities of the controller or the processor involve “regular and systematic monitoring of data subjects on a large scale” or where the entity conducts large-scale processing of “special categories of personal data” (such as that revealing racial or ethnic origin, political opinions, religious or philosophical beliefs)</p>	<p>officer to help demonstrate compliance.</p>	<ul style="list-style-type: none"> • the officer is responsible along with the management for ensuring and monitoring compliance with the Data Protection Policy and the legislation • the officer is able to inform and advise the organisation and other staff with queries on data protection, auditing personal data held and deals with data subject requests • the officer is the first point of contact for reporting a personal data breach. • the officer is involved in a proper and timely manner in all issues relating to personal data • provision of resources to carry out the tasks required • the officer shall have access to personal data and processing operations • the officer is required to maintain their expert knowledge • the officer monitors the assignments of responsibilities within the organisation, awareness- raising and training of staff and audits • provides advice on and monitors data protection impact assessment where applicable to the processing • co-operates, acts as contact point for and liaises with any supervisory authority • the officer has a written job specification and reports direct into the Board/ Senior leadership team/ Trustees
--	--	---

© QG Business Solutions Ltd 2017. This document remains the property of QG Business Solutions Ltd and cannot be changed in any way. You may use this information free of charge, to assess yourself against the requirement of the GDPR Essentials Scheme. This document must not be used in a commercial manner to assist other organisations without the approval of QG Business Solutions Ltd. The document may be reproduced, in any manner in its entirety and distributed to interested parties.

Visit www.qgstandards.co.uk, QG Business Solutions Ltd, Westwinds, Lambley Bank, Scotby, Carlisle, CA4 8BX. 01228 631681 cyber@qgbiz.co.uk