GDPR MANAGEMENT STANDARD

QG-GDPR Management Standard

Requirements for a Managed GDPR System

QG Publication
6th July 17

Rev 6th Nov 17

Rev 11th July 18

Document No.
QG 0201/4.5

GDPR MANAGEMENT STANDARD

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 Fundamentals questionnaire. If you are applying for GDPR Fundamentals PLUS your systems will be audited against these requirements.

GDPR MANAGEMENT STANDARD

QG-GDPR Management Standard

No.	Section	Standard	Deliverables

	Data Protection Policy	A written data protection policy is in place that sets out clearly the legal obligations under data protection legislation.	The policy is to cover the regulations stated in sections 3 – 13 of this document, in writing and must include the details below;
			• management commitment,
			• definitions,
			• the legal principles,
			• data subjects legal rights (including children aged under 13)
			  ○ The right to be informed
			  ○ The right of access
			  ○ The right to rectification
			  ○ The right to erasure
			  ○ The right to restrict processing
			  ○ The right to data portability
			  ○ The right to object
			  ○ Rights in relation to automated decision making and profiling.
			• how to complain
			• dated
			• minimum annual review

			Documents (evidence) Required • Signed Policy Document

2	Management Responsibilities	Management responsibilities are defined in writing	Organisation ownership is defined, in writing and by section • Evidence is in place that individuals understand that they have section responsibility • 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 **Documents (evidence) Required** • Signed training register / roles responsibility description stating section responsibility.
3	Data Protection Objectives	Company data protection objectives are documented, agreed and reviewed	A written system is in place that details; • objectives, • scope • definitions A system is in place that reviews and updates objectives on a regular basis (minimum yearly) **Documents (evidence) Required** • Document register with an expected review date and actual review date (signed)
4	Lawful Basis	The organisation knows what data it holds and what lawful basis it is held for	Organisations are allowed to hold data of individuals under certain conditions, this standard requires for each piece of personal data to be categorised and understood. • **Legal Obligation** processing of Personal Data is necessary for compliance with a legal obligation to which the Controller is subject. • **Vital Interest – (of the data subject)** processing of Personal Data is necessary to protect the vital interest of the data subject or of another data subject • **Public Task – (only applies to public sector)** processing of Personal Data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority • **Contractual Relationship**

			processing of Personal Data is necessary for the performance of a contract to which the data subject is a party or for the Controller to take pre-contractual steps at the request of the data subject • **Legitimate Interest** processing is necessary under the Legitimate Interests of the Controller or Third Party, unless these interests are overridden by the data subject's interests or fundamental rights. • **Consent** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, agrees to the processing of personal data relating to him or her
			Documents (evidence) Required • Records of what legal basis each category of data is held.
5	Collection of Personal Data	Personal data is only collected and processed in compliance with data protection legislation	The organisation has reviewed in the last 12 months • what personal data it holds, • the source of personal data held, • 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

			• assesses which departments/ areas are impacted by the requirements for issuing information notices
			
			The organisation has systems in place for
			
			• When 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;
			  ▪ 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
			  ▪ 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

			• When 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, ▪ 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
			Documents (evidence) Required • 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)
6	Processing Personal Data	Personal data is only processed for the purposes for which it was given and in compliance with the Regulation	The organisation • Undertakes data protection impact assessments (DPIA); ○ on any high risk processing activity before it commences. ○ seeks the views of the affected data subjects or their representatives ○ consults with the supervisory authority if the DPIA identifies a high level of unmitigated risk.

			The organisation has a process in place to • 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. • ensure inaccurate data is erased securely or corrected without delay and any requests for rectification dealt with without undue delay. • 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.
			Documents (evidence) Required • 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	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	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 the organisation; • has implemented appropriate technical and organisational measures such as encryption, pseudonymisation or data minimisation in an effective manner, • regularly test, assess and evaluate the effectiveness of technical and organisational measures for ensuring security and update them where necessary, • endures that 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 • randomly checks to ensure compliance with the requirement to use the appropriate measures • ensures the ongoing confidentiality, integrity, availability and resilience of processing systems and services • are 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 and register ensuring that breaches are notified without undue delay. • has, when using data processors ensure that all arrangements are in signed contractual form • 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 confidentiality statement • 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, confidentially and permanently. • Ensure any contractors used to undertake this task have a signed written contract. • All new technology has privacy by design built in

			Documents (evidence) Required • 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 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	The organisation shall; • have a set procedure for dealing with any data subject access requests, • publish the name and address of the contact to whom such requests should be sent, • make sure public facing staff have been trained and can identify an access request and know where to refer it, • make sure staff know how to verify the identity of the data subject making the request • provide 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 decision which also refers to the next stage of being able to make a complaint to the supervisory authority • keep an internal record of data subject access requests received

			Documents (evidence) Required • 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	The organisation shall; • If a request is received for access to the personal data 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 • if required, provide information in a structured, commonly used and machine readable form, 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.
			Documents (evidence) Required • (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	The organisation will have in place a system that;
			• the data subject is told of their right to object to direct marketing clearly and separately from other information,
			• ensures when a data subject objects to direct marketing, the data is not be used for direct marketing any further,
			• upon a request to restrict processing from a data subject on the basis that
			  ○ 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.

			Documents (evidence) Required • Records of any Data subject that wishes processing to be restricted.

11	Dealing with Requests for Erasure of Data (Right to be forgotten)	Correctly dealing with request to have a data subject's personal data erased.	The organisation will have in place a system that;
			• on receipt of a request, to have personal data erased the organisation will erase such data without undue delay, unless an exemption exists such as
			  ○ right of freedom of expression and information or
			  ○ archiving purposes in the public interest,
			• erase data if it 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 • when the organisation has made the personal data public, erase the data, taking into account available technology and the cost of implementation • takes reasonable steps, including using technical measures itself, to inform other organisations which are processing the data that the data subject has requested erasure
			Documents (evidence) Required • Record of all data requests for the right to be forgotten (erasing info)
12	Use of Profiling and Automated Decision Making	Compliant use of automated individual decision-making including profiling.	The organisation has a system in place • that 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 • to undertake a data protection impact assessment (DPIA) when systematic and extensive automated processing including profiling is required • to undertake necessary regular reviews to assess if processing is performed in accordance with the DPIA • to use appropriate mathematical or statistical procedures to safeguard individuals' rights and freedoms when carrying out automated processing or profiling • so that 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
			Documents (evidence) Required • 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	The organisation has a system in place to • 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. • regularly review key international data flows to ensure compliance with the Regulation • review 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, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available.
			Documents (evidence) Required • 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.	Training is undertaken for all staff both at induction and as annual training and includes: • 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 measures (see section 7) • Internal breach notification procedure • How to identify an access request and who to refer to Staff who process personal data are required to also undertake training in the following areas; • 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
			Documents (evidence) Required • Security Awareness training register signed by individuals
15	Complaints	A system is in place to deal with complaints	A procedure is in place that identifies • 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
			Documents (evidence) Required • 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	A system is in place that reviews ○ Policy ○ Objectives On an annual basis is documented and acted upon
			Documents (evidence) Required • Minutes of management review
17	Audit	An internal and/or third part audit is carried out at regular intervals.	The organisation has a system in place where ○ Random checks are carried out to ensure compliance with the requirements ○ An annual audit is carried out that checks that information held is compliant ○ An audit process is carried out that checks the system at least once per year.
			Documents (evidence) Required • Audit results.


GDPR
MANAGEMENT
STANDARD