CONTENTS IN GDPR DOCUMENTATION TOOLKIT

MANDATORY – Documents that are required under the GDPR
CONDITIONAL OR IMPLIED – Documents that are required under the GDPR only where certain conditions apply or are implied within the context of the requirements
RECOMMENDED – Documents recommended by the ICO or Article 29 Working Party

NO.	DOC NO.	DOCUMENT NAME	MANDATORY	CONDITIONAL OR IMPLIED	RECOMMENDED
	1	**GDPR & TOOLKIT GUIDANCE**			
1	**1.1**	Customisation & Usage Instructions			
2	**1.2**	Toolkit Guidance Document			
3	**1.3**	21-Page GDPR Implementation Project Plan			
	2	**GDPR POLICY DOCUMENTS**			
4	**2.1**	Data Protection Policy & Procedures	**x**		
5	**2.2**	Data Retention & Erasure Policy	**x**		
6	**2.3**	Data Retention Schedule & Periods	**x**		
7	**2.4**	Data Breach Policy & Procedures	**x**		
8	**2.5**	Data Breach Incident Form	**x**		
9	**2.6**	Subject Access Request Procedures & Form	**x**		
10	**2.7**	Data Protection Officer Responsibilities		**x (1)**	
11	**2.8**	International Transfer Procedures		**x (2)**	
	3	**GDPR TEMPLATES & REGISTERS**			
12	**3.1**	Privacy Notice Template	**x**		
13	**3.2**	Employee Privacy Notice Template	**x**		
14	**3.3**	Privacy Notice Register			
15	**3.4**	Information Audit Template			**x**
16	**3.5**	Processing Activities Register		**x (3)**	
17	**3.6**	Processor Agreement Template		**x (4)**	
18	**3.7**	Responses for Subject Access Requests	**x (5)**		
19	**3.8**	Processor Notification Letter			
20	**3.9**	GDPR Compliance Statement Template			
21	**3.10**	Legitimate Interests Assessment (LIA)	**x (6)**		**x**
22	**3.11**	Consent, Parental Consent & Withdrawal Templates		**x (7)**	
	4	**CHECKLISTS & DPIA**			
22	**4.1**	GDPR Compliance Checklist			
23	**4.2**	Information Security Checklist			

24	**4.3**	Complaint Handling Checklist			
25	**4.4**	Data Protection Impact Assessment (DPIA) Procedures		**x (8)**	
26	**4.5**	DPIA Templates in Excel			
	5	**INFORMATION SECURITY**			
27	**5.1**	Information Security Policy		**x (9)**	
28	**5.2**	Access Control & Password Policy			
29	**5.3**	Asset Management Policy			
30	**5.4**	BOYD & Remote Access Policy			
31	**5.5**	Clear Desk Policy			
32	**5.6**	Information Asset Register			
33	**5.7**	Secure Disposal Policy			
34	**5.8**	Business Continuity Plan Template		**x (10)**	
	6	**COMPLAINT HANDLING DOCUMENTS**			
35	**6.1**	Complaint Handling Policy & Procedures			
36	**6.2**	Complaint Handling Form			
37	**6.3**	Complaint Handling Register			
38	**6.4**	Complaint Response Templates Suite			
	7	**RISK ASSESSMENT & MANAGEMENT**			
39	**7.1**	Risk Management Policy & Procedures			**x**
40	**7.2**	Risk Mitigating Action Plan			
41	**7.3**	Risk Register			
	8	**EMPLOYEE TRAINING & DEVELOPMENT TEMPLATES**			
42	**8.1**	Employee GDPR Communication Summary			
43	**8.2**	Training & Development Policy			
44	**8.3**	Employee Training Record			
45	**8.4**	2 x GDPR Employee Test Papers			
46	**8.5**	Training Feedback Form Template			
47	**8.6**	Training & Development Log			
	9	**SUPPORTING POLICIES & TEMPLATES**			
48	**9.1**	Meeting Minutes & Agenda Template			
49	**9.2**	Supplier Due Diligence Questionnaire			
50	**9.3**	Due Diligence Policy			
51	**9.4**	Internal Audit Policy & Procedures			
52	**9.5**	Compliance Monitoring Register			
53	**9.6**	Outsourcing & Supplier Policy & Procedures			
54	**9.7**	Outsourced Functions Register			
55	**9.8**	Confidentiality Agreement Template			

(1) Appointment of a data protection officer and documenting their duties is mandatory where: -

- The processing is carried out by a public authority or body (*except courts acting in judicial capacity*);
- core activities of controller/processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; or
- core activities of controller/processor consist of processing on a large scale of special categories & personal data relating to criminal convictions and offences

(2) Where the controller/processor transfers personal data outside the EU, they are required to ensure that either an adequacy decision or appropriate safeguards are in place in accordance with Article 45

(3) Maintaining records of processing activities is mandatory for controllers and processors: -

- with more than 250 employees; or
- where the processing they carry out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences

(4) Article 28 requires any controller using a Processor to processes personal data on their behalf to have in place a contract or agreement that stipulates the terms and conditions set out in the Article

(5) Responding to Subject Access Requests with the information noted in Article 15 is mandatory where such a request has been received. Our SAR Responses provide templates for disclosing the required information and for rejecting an access request and notification of timeframe extensions

(6) Where using legitimate interests as a legal basis for processing, Recital 47 advises that *"the existence of a legitimate interest would need careful assessment."* Our LIA template has been developed from the ICO and WP29 guidance on such an assessment, which includes the 3-part test

(7) Gaining consent (*or parental consent*) is mandatory where the controller/processor is relying on consent as their legal basis. This template provides examples on how to obtain and record consent, parental consent and withdrawing consent

(8) Article 35 states that *"where processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact".* The Regulation goes on to say that a data protection impact assessment shall in particular be required in the case of: -

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences;
- a systematic monitoring of a publicly accessible area on a large scale

(9) Throughout the GDPR, the term *"appropriate technical and organisational measures"* is used. This relates to policies, procedures, actions, processes, controls, systems and measures that secure and protect personal data, processing activities and by extension, data subjects. The ICO specially state in their *'Security'* GDPR guidelines that this means having Information Security Policies in place.

(10) Article 32(1)c states *"the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident";* which denotes having a BCP or DR in place.