GDPR Auditor Checklist

01/02/2018

The GDPR Auditor Checklist gives you a high-level overview of how well the organisation complies with the GDPR provisions.
The checklist details specific compliance items, their status, and helpful references.
Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Chapter	Article	Description	Applicable	In Compliance	References	Issues
1		**General Provisions**				
1	1	**Subject-matter and objectives**	Yes	Yes	Information Security Policies and Procedures - Applicable Law - GDPR	
1	2	**Material Scope**	Informational	N/A		
1	3	**Territorial Scope**	Yes	Yes	Information Security Policies and Procedures - Applicable Law - GDPR	
1	4	**Definitions**	Informational	N/A		
2		**Principles**				
2	5	**Principles relating to processing of personal data**	No	No	GDPR Compliance Questionnaire - Principles relating to processing of personal data; Evidence of Compliance - Principles Related to Processing of Personal Data	See Risk Treatment Plan
2	6	**Lawfulness of processing**	Yes	Yes	GDPR Compliance Questionnaire - Personal Data Use; Evidence of Compliance - Personal Data	
2	7	**Conditions for consent**	No	No	GDPR Compliance Questionnaire - Personal Data Use; Evidence of Compliance - Personal Data	See Risk Treatment Plan
2	8	**Conditions applicable to child's consent in relation to information society services**	Yes	Yes	GDPR Compliance Questionnaire - Child Consent; Evidence of Compliance - Child Consent	
2	9	**Processing of special categories of personal data**	Yes	Yes	GDPR Compliance Questionnaire - Special Categories of Personal Data; Evidence of Compliance - Special Categories of Personal Data	
2	10	**Processing of personal data relating to criminal convictions and offences**	Informational	N/A		
2	11	**Processing which does not require identification**	Informational	N/A		
3		**Rights of the data subject**				

GDPR Auditor Checklist

01/02/2018

The GDPR Auditor Checklist gives you a high-level overview of how well the organisation complies with the GDPR provisions.
The checklist details specific compliance items, their status, and helpful references.
Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Chapter	Article	Description	Applicable	In Compliance	References	Issues
3	12	**Transparent information, communication and modalities for the exercise of the rights of the data subject**	Informational	N/A		
3	13	**Information to be provided where personal data are collected from the data subject**	No	No	GDPR Compliance Questionnaire - Privacy Policy Review; Evidence of Compliance - Privacy Policy	See Risk Treatment Plan
3	14	**Information to be provided where personal data have not been obtained from the data subject**	No	No	GDPR Compliance Questionnaire - Privacy Policy Review; Evidence of Compliance - Privacy Policy	See Risk Treatment Plan
3	15	**Right of access by the data subject**	Informational	N/A		
3	16	**Right to rectification**	Informational	N/A		
3	17	**Right to erasure ('right to be forgotten')**	Informational	N/A		
3	18	**Right to restriction of processing**	Informational	N/A		
3	19	**Notification obligation regarding rectification or erasure of personal data or restriction of processing**	Informational	N/A		
3	20	**Right to data portability**	Informational	N/A		
3	21	**Right to object**	Informational	N/A		
3	22	**Automated individual decision-making, including profiling**	Informational	N/A		
3	23	**Restrictions**	Informational	N/A		
4		**Controller and processor**				
4	24	**Responsibility of the controller**	Yes	Yes	ISO 27001 Compliance Checklist; Evidence of Compliance - Implementation of Controls from ISO 27001	

GDPR Auditor Checklist

01/02/2018

The GDPR Auditor Checklist gives you a high-level overview of how well the organisation complies with the GDPR provisions.
The checklist details specific compliance items, their status, and helpful references.
Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Chapter	Article	Description	Applicable	In Compliance	References	Issues
4	25	**Data protection by design and by default**	Yes	Yes	ISO 27001 Compliance Checklist; Evidence of Compliance - Implementation of Controls from ISO 27001	
4	26	**Joint controllers**	Informational	N/A		
4	27	**Representatives of controllers or processors not established in the Union**	No	No	GDPR Compliance Questionnaire - Representatives of controllers or processors not established in the Union; Evidence of Compliance - Representative of Controller or Processors not Established in the Union	See Risk Treatment Plan
4	28	**Processor**	Yes	Yes	GDPR Compliance Questionnaire - Processor or Sub-Processor; Evidence of Compliance - Processor or Sub-processor	
4	29	**Processing under the authority of the controller or processor**	Informational	N/A		
4	30	**Records of processing activities**	Yes	Yes	GDPR Compliance Questionnaire - Personal Data Use; GDPR Compliance Questionnaire - Processor or Sub-Processor	
4	31	**Cooperation with the supervisory authority**	Yes	Yes	Information Security Policies and Procedures - Applicable Law - GDPR	
4	32	**Security of Processing**	Yes	Yes	ISO 27001 Compliance Checklist; Evidence of Compliance - Implementation of Controls from ISO 27001	
4	33	**Notification of a personal data breach to the supervisory authority**	Yes	Yes	Information Security Policies and Procedures - Applicable Law - Breach Notification	
4	34	**Communication of a personal data breach to the data subject**	Yes	Yes	Information Security Policies and Procedures - Applicable Law - Breach Notification	
4	35	**Data protection impact assessment**	Yes	Yes	Data Protection Impact Assessment; Evidence of Compliance - Implementation of Controls from ISO 27001	
4	36	**Prior consultation**	Informational	N/A		

GDPR Auditor Checklist

01/02/2018

The GDPR Auditor Checklist gives you a high-level overview of how well the organisation complies with the GDPR provisions.
The checklist details specific compliance items, their status, and helpful references.
Use the checklist to quickly identify potential issues to be re-mediated in order to achieve compliance.

Chapter	Article	Description	Applicable	In Compliance	References	Issues
4	37	**Designation of the data protection officer**	Yes	Yes	Information Security Policies and Procedures - Data Protection Officer; GDPR Compliance Questionnaire - Data Protection Officer	
4	38	**Position of the data protection officer**	Yes	Yes	Information Security Policies and Procedures - Data Protection Officer	
4	39	**Tasks of the data protection officer**	Yes	Yes	Information Security Policies and Procedures - Data Protection Officer	
	40+	*Additional Regulations for Supervisory Authorities, Member States and Certification Bodies*	*No*	N/A		