Gartner

GDPR Audit Checklist

The Gartner GDPR Audit Checklist helps organizations prepare for internal and external audits of GDPR compliance.

Instructions:
1. Track the status of all checklist items until fully compliant.
2. Use the notes page as needed for comments on progress.

For each requirement we have noted the relevant GDPR article for easy reference.

Get Started

Gartner GDPR Audit Checklist

Status key

FC = Fully compliant IP = In progress NC = Not compliant NA = Not applicable

	Audit question	Reference article	Status			
Accountability governance	Do you maintain an overarching data protection policy that demonstrates compliance with requirements including processing, privacy by design and record keeping?	5(2)	FC ○	IP ○	NC ○	NA ○
	Do you train all employees on GDPR requirements and principles — including processing activities, controls, privacy impact assessments, audits, data subject rights, reporting lines and privacy by design — and the potential impact of noncompliance?	5(2)	FC ○	IP ○	NC ○	NA ○
	Do you regularly test, retrain and maintain records of training for employees who handle personal data on their understanding of GDPR requirements?	5(2)	FC ○	IP ○	NC ○	NA ○
	If you require a data protection officer (DPO), does he or she have reporting authority to the highest level of management, necessary resources, independence, and authority to ensure compliance with the GDPR and other data protection laws?	7(1) 38(1-4,6)	FC ○	IP ○	NC ○	NA ○
	Is the DPO bound by secrecy or confidentiality concerning the performance of his or her tasks?	38(5)	FC ○	IP ○	NC ○	NA ○
	If the DPO has other responsibilities, have they been assessed to avoid conflicts of interest?	38(6)	FC ○	IP ○	NC ○	NA ○
	Does the DPO have the knowledge and ability to fulfill tasks outlined in Article 39?	37(5) 39(1,2)	FC ○	IP ○	NC ○	NA ○
	Have you shared the DPO's contact information internally, publicly and with the relevant supervisory authority?	37(7)	FC ○	IP ○	NC ○	NA ○
Processing principles	Do you maintain records management and data retention policies?	24(1,2,3)	FC ○	IP ○	NC ○	NA ○
	Have you documented principles to justify retention periods?	5(1)	FC ○	IP ○	NC ○	NA ○
	Is personal data processed lawfully, fairly and in a transparent manner?	5(1) 6(1,2,3,4)	FC ○	IP ○	NC ○	NA ○
	Is personal data collected for specified, explicit and legitimate purposes, and not further processed in a manner incompatible with those purposes?	5(1)	FC ○	IP ○	NC ○	NA ○
	Is personal data relevant, limited and minimized to what is necessary in relation to the purposes for which they are processed?	5(1)	FC ○	IP ○	NC ○	NA ○
	Is personal data accurate and kept up to date — and is every reasonable step taken to ensure inaccurate personal data is erased and rectified without delay?	5(1)	FC ○	IP ○	NC ○	NA ○
	Is personal data kept only for as long as is necessary for the purposes for which it is processed?	5(1)	FC ○	IP ○	NC ○	NA ○
	Is personal data processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures?	5(1)	FC ○	IP ○	NC ○	NA ○
	Have you clearly identified, detailed, documented and kept up to date the purpose(s) of processing personal data?	5(1)	FC ○	IP ○	NC ○	NA ○
	Have you implemented appropriate technical or organizational measures to ensure security of personal data, including protection against unauthorized processing, accidental loss, destruction or damage?	5(1) 24(1,2)	FC ○	IP ○	NC ○	NA ○
	If you process special categories of sensitive data (revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation), are you in compliance with Article 9(2) conditions?	9(1,2)	FC ○	IP ○	NC ○	NA ○
	If you process personal data relating to criminal convictions and offenses or related security measures based on Article 6(1), is this carried out under the control of official authority or authorized by union or member state law?	10	FC ○	IP ○	NC ○	NA ○

continued on next page

Gartner GDPR Audit Checklist (continued)

Status key

FC = Fully compliant IP = In progress NC = Not compliant NA = Not applicable

	Audit question	Reference article	Status			
Privacy by design and default	Do you ensure processes are in place to embed privacy by design and default into projects, to include measures that ensure data minimization, pseudonymization, encryption and the processing of only personal data necessary for specified purposes?	25(1,2) 32(1,4)	FC ○	IP ○	NC ○	NA ○
	Do you restrict access to personal data to only those employees processing the data?	24(1) 25(1,2)	FC ○	IP ○	NC ○	NA ○
	Do you frequently audit and test systems and services to ensure ongoing confidentiality, integrity, availability and resilience?	32(1)	FC ○	IP ○	NC ○	NA ○
	Do you ensure processes and systems can be restored in the event of physical or technical incidents?	32(1,2)	FC ○	IP ○	NC ○	NA ○
	Do you maintain a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing?	32(1)	FC ○	IP ○	NC ○	NA ○
	Do you apply storage and processing methods (e.g., redaction) to hard copies of personal data?	24(1,2) 25(1,2)	FC ○	IP ○	NC ○	NA ○
	Do you maintain documented data destruction procedures in place for information that is no longer necessary — and do you take steps to ensure employees comply with procedures?	24(1,2) 25(1,2)	FC ○	IP ○	NC ○	NA ○
Data protection impact assessment	Do you carry out a data protection impact assessment (DPIA) whenever the use of new technologies is likely to result in high risk to data subjects, decisions from automated processing have a legal impact, processing involves special categories of data referred to in Article 9(1) or 10, or include large-scale systematic monitoring of publicly accessible areas?	35(1)	FC ○	IP ○	NC ○	NA ○
	Is the DPO always involved when carrying out a DPIA?	35(2)	FC ○	IP ○	NC ○	NA ○
	Does the DPIA contain a systematic description of the envisaged processing operations, the purpose of processing, an assessment of the necessity and proportion of processing in relation to the purposes, an assessment of the risks to rights and freedoms of data subjects, and measures envisaged to address the risks, such as safeguards and security measures?	35(7)	FC ○	IP ○	NC ○	NA ○
	Where appropriate, do you seek the views of data subjects or their representatives on intended processing?	35(9)	FC ○	IP ○	NC ○	NA ○
	Do you have a process in place for detecting changes in risks — and do you review DPIAs for changed risks?	35(11)	FC ○	IP ○	NC ○	NA ○
	Are risks arising from each DPIA mitigated?	36(1,2)	FC ○	IP ○	NC ○	NA ○
	When risks cannot be mitigated, do you contact the supervisory authority with a list of controller and processor responsibilities, the purposes and means of intended processing, measures and safeguards provided to protect data subjects, the DPO's contact details, the DPIA and any other requested information?	36(3)	FC ○	IP ○	NC ○	NA ○
Records of processing	If you are a controller employing more than 250 people or processing types of data listed in Article 30(5), do you maintain a record of processing activities containing the name and contact details of the controller and DPO, the purpose of processing, a description of data subject and personal data categories, categories of recipients to whom personal data have been or will be disclosed, international transfers of data, time limits for data erasure, and a description of technical and organizational security measures in place?	30(1,3,5)	FC ○	IP ○	NC ○	NA ○
	If you are a processor employing more than 250 people or processing types of data listed in Article 30(5), do you maintain a record of processing activities containing the name and contact details of the processor, controller and DPO; categories of processing carried out on behalf of each controller; international transfers of data; and a description of technical and organizational security measures in place?	30(2,3,5)	FC ○	IP ○	NC ○	NA ○
	Do you ensure records of processing activities are maintained in writing and available to the supervisory authority on request?	30(3,4) 31	FC ○	IP ○	NC ○	NA ○

continued on next page

Gartner GDPR Audit Checklist (continued)

Status key

FC = Fully compliant IP = In progress NC = Not compliant NA = Not applicable

	Audit question	Reference article	Status			
Data subject rights	Where a data subject exercises their right of access, do you ensure they are provided with all items listed in Article 15(1)?	15(1,2,3,4)	FC ○	IP ○	NC ○	NA ○
	Do you maintain processes for rectifying inaccurate personal data and having incomplete personal data completed?	16	FC ○	IP ○	NC ○	NA ○
	Where a data subject requests the erasure of personal data, do you take every reasonable step to erase all data, links and copies without undue delay and when Article 17(1) grounds apply?	17(1,2,3)	FC ○	IP ○	NC ○	NA ○
	Where the accuracy of personal data is contested, do you restrict processing to enable verification of accuracy?	18(1,2)	FC ○	IP ○	NC ○	NA ○
	Where processing is no longer necessary or lawful, do you have a process for restricting processing when requested by data subjects?	18(1,2)	FC ○	IP ○	NC ○	NA ○
	Do you ensure data subjects who have obtained restriction of processing are informed before restrictions are lifted?	18(3)	FC ○	IP ○	NC ○	NA ○
	Do you notify all processors and other personal data recipients of rectifications, erasures and restrictions of processing?	19	FC ○	IP ○	NC ○	NA ○
	Where a data subject exercises their right to data portability, do you transmit data to another controller without hindrance, by automated means, and in a common and machine-readable format?	20(1,2)	FC ○	IP ○	NC ○	NA ○
	Where data subjects object to having their data processed for direct marketing, do you no longer process their data?	21(2,3,4)	FC ○	IP ○	NC ○	NA ○
	Where data subjects object to having their data processed for research or official purposes, do you no longer process their data unless you can present compelling legitimate grounds?	21(1,6)	FC ○	IP ○	NC ○	NA ○
	Do you ensure data subjects have the right not to be subject to legal or similarly affecting decisions based on automated processing?	22(1,2,3,4)	FC ○	IP ○	NC ○	NA ○
Consent and notices	Are you able to demonstrate that data subjects have consented to the processing of their data?	7(1)	FC ○	IP ○	NC ○	NA ○
	Are consent requests clearly distinguishable from other matters, in an intelligible and accessible form, and written in clear and plain language?	7(2)	FC ○	IP ○	NC ○	NA ○
	Are data subjects asked to positively opt-in (separate and unticked opt-in boxes per Recital 32)?	7(1,2)	FC ○	IP ○	NC ○	NA ○
	Do data subjects have the right to withdraw consent at any time — and is withdrawing consent as easy and giving consent?	7(3)	FC ○	IP ○	NC ○	NA ○
	Where processing data of subjects below the age of 16 years, is consent given and authorized by the holder of parental responsibility — and are reasonable efforts made to verify this consent?	8(1,2)	FC ○	IP ○	NC ○	NA ○
	Are privacy notices and policies clearly provided to data subjects with processor and DPO contact information, purposes of processing, legal bases for processing, recipients of personal data, international transfers, data retention periods and data subject rights?	13(1,2) 14(1,2)	FC ○	IP ○	NC ○	NA ○
	Where personal data is not obtained directly from data subjects, do you provide categories of personal data and the originating sources and whether those are publicly accessible?	14(2)	FC ○	IP ○	NC ○	NA ○
	Are privacy notices and policies provided to data subjects at the time of collection from data subjects or within one month when not obtained from data subjects?	13(1,2) 14(3)	FC ○	IP ○	NC ○	NA ○
	Are privacy notices and policies provided to data subjects prior to further processing when they have not previously been communicated?	13(3,4) 14(4,5)	FC ○	IP ○	NC ○	NA ○
	Are all communications with data subjects provided in writing using clear, concise and transparent language?	12(1)	FC ○	IP ○	NC ○	NA ○
	Where information on action taken on data subject rights (Article 15-22) cannot be provided within one month of receipt, do you inform data subjects of the required extension within one month, include reasons for the delay, and extend delivery no more than two months?	12(3)	FC ○	IP ○	NC ○	NA ○
	If you do not take action on requests of the data subject, do you inform the data subject of reasons for not taking action, without delay and within one month of receipt, and include possibilities for lodging complaints with a supervisory authority or seeking judicial remedy?	12(4)	FC ○	IP ○	NC ○	NA ○
	Are information requests provided free of charge unless demonstrated by the controller to be manifestly unfounded or excessive?	12(5)	FC ○	IP ○	NC ○	NA ○

continued on next page

Gartner GDPR Audit Checklist (continued)

Status key

FC = Fully compliant IP = In progress NC = Not compliant NA = Not applicable

	Audit question	Reference article	Status			
Breach management	Do you maintain breach incident and notification policies and procedures?	24(1,2,3) 33(1,2,3,4) 34(1,2,3)	FC ○	IP ○	NC ○	NA ○
	Are security measures (e.g., backup, pseudonymization, encryption, testing) implemented and appropriate for data risks?	32(1)	FC ○	IP ○	NC ○	NA ○
	Do you have an up-to-date data breach response plan?	33(1,2,3,4)	FC ○	IP ○	NC ○	NA ○
	Do you investigate and take corrective action for all personal data breaches regardless of size or scope?	33(1)	FC ○	IP ○	NC ○	NA ○
	For breaches likely to result in a risk to data subjects, do you report the breach to the supervisory authority within 72 hours with categories and the number of subjects concerned, the categories and number of data records concerned, the DPO's contact information, the likely consequences of the data breach, and measures proposed or taken to address the breach?	33(1,3)	FC ○	IP ○	NC ○	NA ○
	If you are a processor, do you notify the controller without undue delay after becoming aware of a data breach?	33(2)	FC ○	IP ○	NC ○	NA ○
	Do you maintain a data breach register including facts related to the breach, effects and remedial actions taken?	33(5)	FC ○	IP ○	NC ○	NA ○
	Do you communicate breaches to affected data subjects without undue delay and in clear and plain language?	34(1,2)	FC ○	IP ○	NC ○	NA ○
Processors	Do you maintain policies and procedures for contracting and conducting due diligence on processors and subprocessors?	24(1,2,3)	FC ○	IP ○	NC ○	NA ○
	Do you only use processors that ensure protection of data subject rights using appropriate technical and organizational measures?	28(1)	FC ○	IP ○	NC ○	NA ○
	If you are a processor, do you not engage with other processors without prior specific and general written authorization from the controller?	28(2)	FC ○	IP ○	NC ○	NA ○
	Are all processors governed by a contract that establishes the subject matter of processing, duration of processing, nature and purpose of processing, type of personal data and categories of data subjects, and obligation and rights of the controller?	28(3)	FC ○	IP ○	NC ○	NA ○
	Do contracts and service level agreements with processors outline international data transfers restrictions, ensure confidentiality from persons processing personal data, ensure deletion or return of personal data to controllers at the end of services, allow controllers and auditors to obtain information necessary for inspections and audits, and include all Article 32 security measures?	28(3)	FC ○	IP ○	NC ○	NA ○
	Do processors ensure data protection by design and default in all processing activities?	25(1) 28(1)	FC ○	IP ○	NC ○	NA ○
Data transfers	When transferring or disclosing personal information, do you encrypt data and only send necessary data?	32(1)	FC ○	IP ○	NC ○	NA ○
	Do you use secure data transfer methods for all communications (e.g., email, file transfers, website forms, payments)?	32(1)	FC ○	IP ○	NC ○	NA ○
	Have you identified all international data flows and export mechanisms?	44	FC ○	IP ○	NC ○	NA ○
	Are international data transfers authorized by the Commission (Article 45) or appropriately safeguarded in addition to preserving data subject rights and legal remedies (Article 46)?	45(1) 46(1,2)	FC ○	IP ○	NC ○	NA ○
	Do you regularly check the Official Journal of the European Union for the commission's withdrawals and changes to data transfer authorizations?	45(8)	FC ○	IP ○	NC ○	NA ○
	Are appropriate data transfer safeguards provided for by contractual clauses or provisions inserted into administrative arrangements?	46(3)	FC ○	IP ○	NC ○	NA ○
	When relying on binding corporate rules for data transfers, do you ensure they are legally binding and apply to and are enforced by every member concerned of the group of undertakings, in addition to expressly conferring enforceable rights on data subjects with regard to the processing of their personal data?	47(1)	FC ○	IP ○	NC ○	NA ○
	Do binding corporate rules specify all items in Article 47(2)?	47(1,2)	FC ○	IP ○	NC ○	NA ○

continued on next page

GDPR Checklist Notes

Gartner provides legal and compliance leaders with indispensable insights, advice and tools to achieve their mission-critical priorities and position their organization for growth.

Contact us to learn more about how we can help you manage your compliance and privacy risks.

Contact us

Phone: 1 800 213 4848
Email: legalcomplianceleaders@gartner.com
Web: gartner.com/go/legal-compliance

Gartner®