

GDPR compliance



Company
GDPR AIC
Certification



3 steps to the full **AIC** certification for companies

Assessment

- ✎ Detect control gaps in current processes and policies to comply with the GDPR
- ✎ Prioritize actions to address gaps based on **real** business risks
- ✎ Detect where **critical** personal data is stored and its security controls

Implementation

- ✎ Design, improve and explain policies
- ✎ Simplify and facilitate changes across departments
- ✎ Reinforced security controls aligned to ISO 27001
- ✎ Develop the skills for the people dealing with privacy risks

Conclusion

- ✎ Obtain the final certification

The GDPR Institute



Independent approach

Based on






- Rules by the Justitsministeriet
 - model for good data protection practices
 - draft developed by DK Datatilsynet
- Best practices and benchmark against ISO 27001
 - focused on preventing a data breach
 - change management
- Trusted advisor
 - facilitation role to close gaps
 - independent from software solution providers

A	B	C	D	E	F	G
Chapter	Department	Article	Control goal	control activity	documentation	Example of the audit procedure
4. the data controller and data processor	Section 1 - General obligations	28 - Data Processor 29 - treatment carried out for the controller or the processor	data controller and the data processing undertaken solely by processors approved by the controller.	28.3 The data controller has authorized data processor using other processors.	Evidence of the use of other data processors authorized by the data controller	28.3.1 Review the evidence that the controller has accepted the use of other processors
4. the data controller and data processor	Section 1 - General obligations	28 - Data Processor 29 - treatment carried out for the controller or the processor		4.28 Management is entitled to the processing and protection of personal data with other data processors are made in accordance with instructions from the controller.	Documentation for management approval of the processing of personal data is done in accordance with the instructions, including checks of the data processing of other therapists	28.4.1 Review the documentation that management has ensured that the processing and protection of personal data with other data used therapists are done in accordance with the instructions
30 - Inventory of processing operations						
4. the data controller and data processor	Section 1 - General obligations	30 - Inventory of processing operations		30.1 The data controller has authorized the contents of the register both to the processing activities of the controller.	List of processing activities in written / electronic form	30.1.1 Review the documentation of the existence of a list of the processing operations for each controller.
4. the data controller and data processor	Section 1 - General obligations	30 - Inventory of processing operations		30.2 The data controller has authorized the contents of the register both to the processing activities of the controller.	Documentation that the plan approved by the individual controllers	30.2.1 Review the documentation for the controller has authorized the contents of the register both to the processing activities of the controller.
4. the data controller and data processor	Section 1 - General obligations	30 - Inventory of processing operations	There compliance procedures and controls to ensure that the data controller keeps a register of the processing of personal information that is under its responsibility.	3.30 There is performed regularly - and at least once a year - assessment of whether the inventory is updated and correct.	Evidence of management's consideration and approval of the updated list.	30.3.1 Review the evidence that the inventory of processing operations for each controller is updated and correct.
4. the data	Section 1 -	30 - Inventory of processing		4.30 Management has ensured that the	Evidence of management's	30.4.1 Review the

Specimen




Expertise in

Consultancy and control implementation

-  The GDPR roadmap: simple and practical multidisciplinary approach
-  Templates for a privacy program: set of policies and tools
-  Data Protection Impact Assessment
-  Gap analysis
-  Data security, business continuity, resilience and IT governance

Training

Certification

-  FAS Foundation, Application and Substance
-  AIC Corporate Certification
-  DPO course



How we demonstrate
compliance?

Easy documentation



“If something is not documented, it is not done”



- My auditor

Extensive documentation efforts for GDPR

Discussions about the right level of documentation

Formalizing operational procedures

Need to integrate privacy practices in policies

Data Controllers must be able to prove their compliance with the GDPR under the accountability principle and upon request of Supervisory Authority

Objectives



Management

- ✦ Privacy is part of the general management system
 - ✦ Documentation is the evidence of accountability and good governance
- ✦ Privacy policy
 - ✦ Supported by: document retention and destruction, info classification, breach management,...
 - ✦ Assess and manage the impact of changes in policies
 - ✦ Available to all the staff (training)

Corporate defense

- ✦ Demonstrate compliance efforts (implementation measures, control improvement)
 - ✦ Records of processing activities under your responsibility (art. 30)
 - ✦ When needed, data protection impact assessment (art. 35)
 - ✦ Records of consent from data subjects and guardians (arts. 7 and 8)
 - ✦ Actions taken during a data breach (arts. 33 and 34)
 - ✦ Purposes for collecting information (art. 13)
- ✦ Document legal basis for the processing (art. 5)
- ✦ Privacy clauses in contracts, bidding corporate rules,...



Audits

- ✦ Outsourcer/data processor must prove technical and organizational controls (art. 28, ISAE 3000 type 1, data protection seals and certifications)

Privacy governance



17	18 - Right to limitation of treatment		(X)	X	X
18	19 - Obligation to communicate information in connection with correction or removal of personal data, or limitation of treatment	Control objectives in artikel 19 are covered under Articles 16, 17 and 18			
19	20 - Right to data portability	(X) Handling of physical media	X	X	X
20	21 - Right to object 22 - Automated individual decisions, including profiling	The requirements are covered by the control objectives in Article 6			
21	23 - Limitations	N / A - the area is not relevant to gauging a statement			
22	24 - The controller's responsibility 25	(X) Handling of physical media	X	X	X
23	26 - Common controller 27 - Representatives of data controllers and data processors who are not established in the Union	N / A - areas are not relevant to gauging a statement			
24	28 - Data Processor 29 - treatment carried out for the controller or the processor	X	X	X	X
25	30 - Inventory of processing operations	X	X	X	X
26	31 - Cooperation with regulator	N / A - the area is not relevant to gauging a statement			
27	32 - Treatment Safety		X	X	X
28	33 - Notification of a personal data breach to the supervisory authority 34 - Notification of a personal data breach to the data subject	X	X	X	X
29	35 - Impact assessment on data protection	X	X	X	X
30	36 - Prior consultation	X	X	X	X
31	37 - Data Protection Advisor	X	X	X	X
32	38 - Data Protection Consultant's position	X	X	X	X
33	39 - Data protection adviser's duties	X	X	X	X
34	40 - Codes of conduct 41 - Control of authorized codes of conduct 42 - Certification 43 - Certification bodies	N / A - areas are not relevant to gauging a statement			
	44 - General principle of the transfer 45 - Transfer based on a decision on the adequate protection level 46 - Transfers subject to appropriate safeguards 47 - BCRs 48 - Transfer or	(X) Handling of physical media	X	X	X

Specimen

Demonstrate compliance



- ✎ Evidence of board engagement in privacy (art. 5)
 - ✎ Unclear evidence: approving a privacy program, board agendas and minutes covering GDPR issues, evaluation of privacy reports, action plans involving board members, list of project stakeholders, budgets, approval
 - ✎ Nice to have: job roles assigning privacy responsibilities, privacy core team and experts, meetings and guidance with other internal functions dealing with personal data
 - ✎ General: ISO/IEC 27001 compliance certificate



Demonstrate compliance



- ✎ If required, board minute designating a DPO (art. 37, 38)
 - ✎ including evidence of independent reporting (org. chart, reports to the board), delegated tasks (contract, job description), proper budget, qualifications and certifications (CV, identity and background checks) and communication to supervisory authority
- ✎ For non-EU data controllers/processors, mandate to designate a representative in the EU and external communication in privacy notes and website (art. 27)
 - ✎ Privacy Officer, Privacy Counsel, CPO, Representative

Operational privacy



7	5 - Principles of processing of personal data	(X) Handling of physical media	X	X	X
8	6 - legality treatment		X	X	X
9	7 - Conditions for consent 8 - Conditions for a child's consent in relation to information society services			(X)	X
10	9 - Special categories of personal data 10 - Processing of personal data relating to criminal convictions and offenses	(X) Handling of physical media	X	X	X
11	11 - The treatment that does not require identification			X	X
12	12 - Transparent information, communications and procedures for exercising the data subject's rights			X	X
13	13 - Information in cases of collection of personal data from the data subject 14 - Disclosure if personal data is not collected from the data subject			(X)	X
14	15 - The data subject's right of access				X
15	16 - Right of reply		(X)	X	X
16	17 - Right of erasure ("right to be forgotten")		(X)	X	X
17	18 - Right to limitation of treatment		(X)	X	X
19	19 - Obligation to communicate information in connection with correction or removal of personal data				

specimen

Control objectives in artikel 19 are covered under Articles 16, 17 and 18

Demonstrate compliance



Principles (art 5)

- ✎ A data privacy policy approved by top management
 - ✎ Integrated with the data security policy
 - ✎ Addressing privacy principles, lawfulness, purpose limitation, transparency, data minimization, accountability, deletion after use quality integrity and confidentiality
 - ✎ Mechanisms to maintain the data quality: data owner
 - ✎ Annually updated
- ✎ Supporting privacy policies
 - ✎ Code of conduct including privacy, staff handbooks, use of IT assets, information classification, document retention, document destruction, marketing
- ✎ DPIAs for new or changing programs, systems, processes

Lawfulness of processing (art 6)




- ✎ DPIAs for new or changing programs, systems, processes
- ✎ Contracts and data processing agreements with 3rd parties details the legal reasons for processing
- ✎ Procedure for secondary uses of personal data
 - ✎ How to manage personal information for other purposes other than it was originally collected
 - ✎ Mechanism for de-identifying data (art 89) for archiving purposes in the public interest, or scientific and historical research purposes, or statistical purposes

Processing of special categories of personal data (art 9) and criminal convictions and offences (art 10)

- ✎ Policy for collection and use of sensitive personal data
 - ✎ How to document legal basis for processing sensitive data contract, vital interests
 - ✎ How to identify racial or ethnic origin, political opinions, biometric data
 - ✎ Controls linked to the data classification policy
 - ✎ Ensure the specific written consent
 - ✎ Contact clauses limiting processed after prior instructions from the controller

Consents (arts 7 and 8)

Procedure to obtain valid consents

-  Consents are gotten before processing data
-  Relevance, clear and plain language, simplicity and accessibility
-  Define who is responsible for controlling that processing is consistent with consents

Procedures to respond to requests to opt-out of, restrict or object to processing

-  Effectively stop processing, responsible person, response actions

Procedure for children's consents

-  How to verify parents/guardians

Transparent information (arts 12, 13 and 14)

- ✎ Procedure to obtain valid data privacy notices
 - ✎ Effective communication of how to exercise the rights of the data subject
 - ✎ Notices are gotten before collecting data
 - ✎ Define the mechanisms
 - ✎ statements, icons, pop-up notifications, scripts
 - ✎ Who approves and control the notices (legal knowledge)
 - ✎ Define who is responsible for controlling that processing is consistent with notices and the description of activities is accurate
- ✎ Protocol for a data breach notification
 - ✎ to affected individuals, to regulators, credit agencies, law enforcement

Demonstrate compliance



Right of access (art 15)





Also managed for: **rectification** (art 16) **erasure** (art 17) **restrict processing** (art 18) **update** (art 19) **portability** (art 20) **object** (art 21) **limit profiling** (art 22)

Subject Access Request procedure and similar




Define the channels

-  email, online form, in writing

Formalize who is responsible for responding (on time)

-  who is authorized to access data to respond
-  coordinating with other operative units
-  cover internal data and external data used by other processors and third parties
-  KPI reports (number of request, complains, explanations of root causes)

Define who controls/approves the final action

-  copy, modification, deletion, restriction
-  confirm that the required action is correct (on the event and periodic monitoring)
-  minutes of management meetings justifying any refusal

Manage privacy risks








		5 - Principles of processing of personal data				
2: Principles	REACH	5 - Principles of processing of personal data		5.1 There are written procedures, which is updated at least annually, taking into consideration the following principles for the processing of personal data: - legality, fairness and transparency - purpose limitation - data minimization - reliability - storage limitation - the integrity and confidentiality.	Written procedures for the processing of personal data.	5.1.1 Review of written procedures for processing of personal data to ensure that they are updated and includes principles for handling personal information.
2: Principles	REACH	5 - Principles of processing of personal data	There compliance procedures and controls to ensure that collection, processing and storage of personal information is in accordance with the principles of processing of personal data.	5.2 There are performed regularly - and at least once a year - the assessment of the principles for the processing of personal data is respected and this assessment is documented.	Documentation for the assessment of compliance with the principles of the processing of personal data.	5.2.1 Review the documentation for assessment of principles for processing personal data to ensure that at least annually, a judgment is made of principles for processing of personal data and respect for them.
2: Principles	REACH	5 - Principles of processing of personal data		5.3 Management have considered and approved the assessment of compliance with the principles for the processing of personal data, including control of other used processors.	Documentation for management approval of the assessment of compliance with the principles for the processing of personal data - eg. The minutes of management meeting.	5.3.1 Review the documentation for management approval of the assessment of compliance with the principles of the processing of personal data.
		6 - legality treatment				
2: Principles	REACH	6 - legality treatment		6.1 There are written procedures, which is updated at least annually, and containing requirements for lawful processing of personal data by the processor.	Written procedures for the processing of personal data.	6.1.1 Review of written procedures for the processing of personal information to ensure that they are updated and contains requirements for lawful processing of personal data.
2: Principles	REACH	6 - legality treatment		6.2 There is one of the controller approved processor agreement, etc., Which contains a summary of what the basic processing of personal data is carried out.	Summary of the basis for the processing of personal data for the individual responsible for the data - eg. Included in the contract, data processing agreement similar.	6.2.1 Review the documentation on which basis the processing of personal data carried out and that this is accepted by the controller (processor agreement, etc.).
2: Principles	REACH	6 - legality treatment		6.3 There are performed regularly - and at least once a year - updates of the data controls, approved summary of the basis for the processing of personal data, including the contract, data processing agreement similar.	Summary of the basis for the processing of personal data for the individual responsible for the data - eg. Included in the contract, data processing agreement similar.	6.3.1 Review the documentation for the basic processing of personal data is updated and approved by the controller at least once a year.
2: Principles	REACH	6 - legality treatment	There compliance procedures and controls to ensure that collection, processing and storage of personal information is in accordance with the principles of processing of personal data.	6.4 There are performed regularly - and at least once a year - updates of the data controls, approved summary of the basis for the processing of personal data, including the contract, data processing agreement similar.	Documentation for management approval of the assessment of compliance with the requirements for the lawful processing of personal data, including control of other used processors.	6.4.1 Review the documentation for ongoing assessment that there is or has been unlawful processing of personal data and the Review that this assessment is performed at least annually.
2: Principles	REACH	6 - legality treatment		6.5 Management have considered and approved the assessment of compliance with the requirements for the lawful processing of personal data, including control of other used processors.	Documentation for management approval of the assessment of compliance with the requirements for the lawful processing of personal data - eg. The minutes of management meeting.	6.5.1 Review the documentation for management approval of the assessment of compliance with the requirements for the lawful processing of personal data.

specimen



Responsibility of the controller (art 24)

Formal privacy program

-  Evidence of accountability in GDPR compliance
-  Evidence of activities in managing privacy
 -  implementing effective privacy measures and controls
 -  safeguarding the rights of data subjects
-  Privacy risk assessment across the organization

Link to the data privacy policy

Contingency plans

-  Scenario planning, documented actions for breaches
-  Documented and tested!

Responsibility of the controller; outsourcing (art 28)

- ✎ Clear instructions from the controller to the processor
 - ✎ Document how they are given and how they are accepted
- ✎ Annual review contracts with third party data processors
 - ✎ Approval of a privacy expert (or DPO)
 - ✎ Use of an approved contract template or approve exceptions
 - ✎ Tip: document the meetings with vendors when discussing privacy issues
- ✎ Maintain data privacy requirements for third parties
 - ✎ clients, vendors, processors, affiliates
- ✎ Due diligence and audits for data privacy and security
 - ✎ posture of potential vendors and current processors
 - ✎ evidence that the controller adopted/will adopt effective technical measures
- ✎ Controls for subsequent outsourcing

Records of processing activities (art 30)

- ✎ Can be linked to the data inventory
- ✎ List of all processing activities
 - ✎ Where, type of data, type of processing by third parties, cross border data transfers
- ✎ Evidence of updates
- ✎ Approve the inventory of data managed by controllers



Data transfers (arts 45 to 49)

- ✎ Records of the transfer mechanism used for cross-border data flows
 - ✎ standard contractual clauses, binding corporate rules, EU-US privacy shield, approvals from regulators
 - ✎ authorized transfer (e.g. consent, performance of a contract, public interest)
 - ✎ linked to the data inventory



Security of processing (art 32)

- ✎ User management policy
 - ✎ role-based access, segregation of duties
 - ✎ defined responsible for approving access rights
- ✎ Technical security measures
 - ✎ intrusion detection, firewalls, monitoring, encrypt personal data
- ✎ Review of user accesses and security measures
- ✎ Confidentiality and privacy provisions in employment/vendor contracts
- ✎ Internal security audits and mitigation responses

Data protection impact assessment (arts 35 and 36)

- ✎ DPIA guidelines and templates
- ✎ Consultation to all stakeholders
- ✎ Follow-up of action plans for detected risks
 - ✎ Evidence of monitoring for closing issues
 - ✎ Changes to systems and controls are tested as effective
- ✎ Eventual consultation to the supervisory authority



Data breach notification (art 33)

- ✎ Data privacy incident or breach response plan
- ✎ Monitoring of abnormal data activity (e.g. downloads)
- ✎ Escalation procedures involving the privacy expert
- ✎ Protocols for
 - ✎ Breach notification to affected individuals
 - ✎ Breach reporting to regulators, credit agencies, law enforcement
- ✎ Log of incidents with forensic analysis
- ✎ Periodic testing / simulation
- ✎ Insurance



Demonstrate compliance



Privacy by design and by default (art 25)

✎ PIA policy for

✎ new or

✎ changes to existing

} programs, systems, or processes

✎ Integrated into system development and business processes

✎ Access controls to least privilege

✎ Involvement of a privacy expert (or DPO)

✎ Assess the risk of affecting data subject rights

✎ Assess technical measures (pseudonymisation)



Useful GDPR links



<https://www.privacyshield.gov/article?id=Privacy-Policy-FAQs-1-5>

- **GDPR Official Text (English, pdf)**
<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
- **EU GDPR Home Page**
<http://ec.europa.eu/justice/data-protection/>
- **Working Party 29 Guidance**
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
- **Guidelines on “Right to Portability” (pdf)**
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf
- **Guidelines on Data Protection Officers (pdf)**
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
- **Guidelines for identifying a controller or processor’s lead supervisory authority (pdf)**
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf
- **Datatilsynet DK Oversight**
<https://www.datatilsynet.dk/forside/>
- **UK ICO – 12 Steps to take now (pdf)**
<https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf>
- **EUGDPR INSTITUTE**
<http://www.eugdpr.institute/faq/>
<http://www.eugdpr.institute/gdpr-thought-leadership/>



Copyright notice



The IP and copyright of this presentation belongs to Copenhagen Compliance®. None of this presentation, either in part or in whole, in any manner or form, may be copied, reproduced, transmitted, modified or distributed or used by other means without explicit permission from Copenhagen Compliance®. Carrying out any unauthorized act in relation to this copyright notice may result in both a civil claim for damages and criminal prosecution.

info@copenhagencompliance.com



As ever, always have your legal advisors review and advise on GDPR or on any contractual obligation. EUGDPR Institute is neither a Law Firm nor are we licensed to provide legal advice.