

GOVERNANCE DOCS

EU General Data Protection Regulation

Gap Assessment Report

EU General Data Protection Regulation (Regulation (EU) 2016/679)

Lindqvist Online Pharmacy (sample)

Processing of customer, prescription and employee data across the online pharmacy and its fulfilment centre.

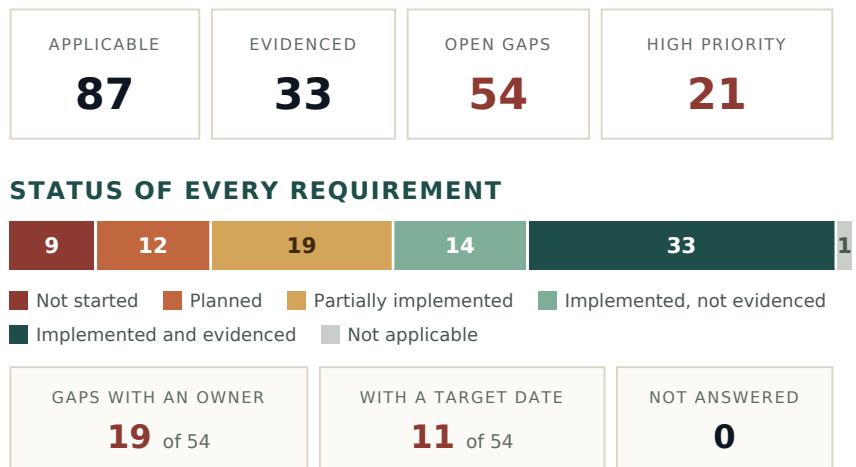
ASSESSED	25 September 2026
EDITION	Regulation (EU) 2016/679
IN SCOPE	88 requirements, 87 applicable
PROFILE	Healthcare and life sciences · 50 to 249 people
PREPARED BY	Governance Docs

CONTENTS

- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Lindqvist Online Pharmacy (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Lindqvist Online Pharmacy (sample) stands against GDPR



WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 64.4% against GDPR across 87 applicable controls. 33 of them are implemented and evidenced.
- Most open gaps: Principles and lawful basis, with 10 at 54%. Strongest area: Records of processing at 94%.
- 14 controls are operating but not evidenced. Collecting their records alone lifts the score to 68.4% (+4.0 points), the cheapest gain available.
- 21 gaps are high priority (not started or only planned); 5 of them are in Principles and lawful basis.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 5 high-priority gaps in Principles and lawful basis	Operations Manager	Procedure for Managing Data Subject Rights
2	MEDIUM	Adopt and tailor the GDPR Roles and Responsibilities, which closes 7 open gaps	To assign	GDPR Roles and Responsibilities
3	LOW	Evidence the 14 controls that already operate (+4.0 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

You hold a 64.4% readiness score at Developing level, and your critical next move is appointing your data protection officer.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

Our self-assessment places us at a 64.4% readiness score at the Developing readiness level, with 54 open gaps across 87 applicable requirements. Our primary exposure sits in governance, specifically the unassigned Data protection officer role and unverified vendor contracts. We request executive approval to formally appoint a data protection officer and assign operational owners to all 21 high priority gaps. Leadership backing ensures resource allocation across business units to formalize accountability and vendor oversight over the next 90 days.

WHERE YOU STAND

Your self-assessment shows an overall readiness score of 64.4%, placing you at level 2 of 4, named Developing. Across 87 applicable requirements, you have 54 open gaps, including 21 high priority gaps. Currently, 33 requirements are implemented and evidenced, 14 are implemented without evidence, 19 are partially implemented, 12 are planned, and 9 are not started. Data protection officer at 15% and Processors and third parties at 41.7% represent your lowest scoring areas.

WHAT IT MEANS FOR THE ORGANIZATION

The assessment highlights operational progress alongside notable governance exposures across your organization. Only 19 open gaps have an assigned owner and only 11 carry a target date. While operational areas like Records of processing reach 93.8%, core oversight mechanisms remain unassigned. Managing personal data without designated governance roles or verified vendor assurances leaves day-to-day operations exposed to compliance breakdowns. Evidencing currently operating controls lifts your score to 68.4%, while completing partially implemented controls reaches 79.3%.

WHERE TO FOCUS FIRST

Focus immediate resources on the 21 high priority gaps, beginning with the Data protection officer requirements and third-party processor controls. Formally designating an officer and defining operational tasks establishes accountability across teams. Securing processor due diligence and audit terms will address critical third-party risks. Prioritize adopting foundational templates such as GDPR Roles and Responsibilities and the Data Protection Policy, which directly resolve multiple open gaps. Transitioning planned items into execution will move the overall score toward 89.7%.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Designate and resource the data protection officer Art 37(1) Designating a data protection officer · Art 38(1) Involving and resourcing the DPO · Art 39 DPO tasks	Operating without an appointed data protection officer leaves core governance obligations unfulfilled and holds the area score at 15%. This gap creates material exposure across healthcare personal data operations.	Define formal responsibilities and reporting lines using the established roles framework.	GDPR Roles and Responsibilities GDPR Toolkit - 100+ Comprehensive Templates	30 DAYS
2 Establish processor due diligence and audit controls Art 28(1) Processor due diligence · Art 28(3)(h) Audit and inspection rights	External processors currently handle personal data without structured assessments or verified audit rights, leaving the area score at 41.7%. Weak supplier verification exposes operations to third-party non-compliance.	Review all active third-party contracts against standard processor assessment criteria.	Processor GDPR Assessment Procedure GDPR Toolkit - 100+ Comprehensive Templates	60 DAYS
3 Formalize controller responsibility and accountability frameworks Art 24 Controller responsibility and measures · Art 5(2) Accountability	Lacking documented controller measures prevents leadership from demonstrating accountability across business functions. Implementing structured policies establishes required organizational safeguards and oversight.	Draft and publish the foundational data protection policy for operational management.	Data Protection Policy GDPR Toolkit - 100+ Comprehensive Templates	60 DAYS
4 Implement procedures for individual erasure and objection rights Art 17 Right to erasure · Art 21 Right to object	Gaps in handling erasure and objections risk improper handling of individual requests. Documented workflows ensure consistent and legally sound responses within operational units.	Standardize internal intake forms and request handling criteria across administrative teams.	Procedure for Managing Data Subject Rights GDPR Toolkit - 100+ Comprehensive Templates	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS - Designate the data protection officer and publish organizational roles and responsibilities. - Assign designated operational owners and delivery targets to all 21 high priority gaps. - Begin gathering documentation to evidence the 14 controls that are already operating.	DAYS 31 TO 60 - Institute standard due diligence reviews and audit terms for all external data processors. - Approve the overarching data protection policy and update the enterprise risk register. - Standardize procedures to ensure personal data accuracy and legitimate basis verifications.	DAYS 61 TO 90 - Operationalize formal fulfillment procedures for data subject erasure and objection requests. - Deliver general data protection awareness training presentations across all departments. - Conduct transfer impact assessments for personal data flows directed to international entities.
---	---	---

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Scope and accountability	2 1 2 1 2	50%	3 2 1
Principles and lawful basis	3 2 3 2 4	54%	5 3 2
Transparency and notices	3 2 2	71%	0 3 2
Data subject rights	2 2 5	66%	3 2 1
Records of processing	1 3	94%	0 0 1
Processors and third parties	3 2 1	42%	3 2 1
Data protection by design and security	1 2 2 3	72%	1 2 2
Personal data breaches	1 1 4	88%	0 1 1
DPIA and prior consultation	2 4	92%	0 0 2
Data protection officer	3 1 1	15%	4 1 0
International transfers	1 3 3	68%	1 3 0
Governance and assurance	1 1 3 1	80%	1 0 1

Not started
Planned
Partially implemented
Implemented, not evidenced
Implemented and evidenced
Not applicable

WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.

Today		64.4%
Evidence what already runs 14 requirements		68.4% +4.0
Finish what is partly in place 19 requirements		79.3% +10.9
Implement what is planned 12 requirements		89.7% +10.4
Start what has not begun 9 requirements		100.0% +10.3

DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.

GDPR Roles and Responsibilities		7
Data Protection Policy		6
Information Security Policy		5
Compliance Evidence		4
Internal Data Protection Policy		4
Risk Register		4

All of these are in the GDPR Toolkit (87 documents).

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 9

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
Art 3	Territorial scope	Scope and accountability	To assign	GDPR Readiness Statement · GDPR Implementation Guide
Art 24	Controller responsibility and measures	Scope and accountability	To assign	Data Protection Policy · Internal Data Protection Policy +1 more
Art 5(1)(d)	Accuracy	Principles and lawful basis	To assign	Procedure for Managing Data Subject Rights · Data Protection Policy
Art 5(1)(f)	Integrity and confidentiality	Principles and lawful basis	Operations Manager 21 Jan 2027	Information Security Policy · Risk Register
Art 8	Children's consent	Principles and lawful basis	IT Manager	Procedure for Consent Management · Consent Request Form
Art 17	Right to erasure	Data subject rights	Risk Manager 21 Jan 2027	Procedure for Managing Data Subject Rights · Retention Policy
Art 37(1)	Designating a data protection officer	Data protection officer	To assign	GDPR Roles and Responsibilities · Internal Data Protection Policy
Art 38(1)	Involving and resourcing the DPO	Data protection officer	To assign	GDPR Roles and Responsibilities · Internal Data Protection Policy
Art 39	DPO tasks	Data protection officer	To assign	GDPR Roles and Responsibilities · GDPR Competence Development Procedure

HIGH Planned · 12

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
Art 5(2)	Accountability	Scope and accountability	To assign	GDPR Documentation Log · Compliance Evidence +1 more
Art 5(1)(a)	Lawfulness, fairness and transparency	Principles and lawful basis	To assign	Data Protection Policy · Personal Data Analysis Procedure

Art 5(1)(b)	Purpose limitation	Principles and lawful basis	To assign	Records of Processing Activities · Procedure Register of Processing Activities
Art 21	Right to object	Data subject rights	To assign	Procedure for Managing Data Subject Rights · Legitimate Interest Assessment Procedure
Art 23	Restrictions under national law	Data subject rights	Risk Manager	Data Subject Request Procedure · Compliance Evidence
Art 28(1)	Processor due diligence	Processors and third parties	Compliance Lead	Processor GDPR Assessment Procedure · Processor GDPR Assessment +1 more
Art 28(3)(h)	Audit and inspection rights	Processors and third parties	To assign	GDPR Contract Review Tool · Processor GDPR Assessment
Art 31	Cooperation with the supervisory authority	Processors and third parties	Risk Manager 7 Jan 2027	Guidance on Engagement with Data Protection Authorities · GDPR Roles and Responsibilities
Art 32(1)(c)	Restoring availability after an incident	Data protection by design and security	To assign	Information Security Policy · Records Retention and Protection Policy
Art 37(7)	Publishing and notifying DPO contact details	Data protection officer	To assign	General Privacy Policy · GDPR Roles and Responsibilities
Art 45	Adequacy decisions	International transfers	IT Manager	Procedure for International Transfers of Personal Data
Art 39(training)	Awareness and training	Governance and assurance	HR Manager	Information Security Awareness Training · GDPR Awareness Training Presentation +1 more

MEDIUM Partially implemented · 19

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
Art 4(7)	Controller and processor roles	Scope and accountability	Operations Manager	GDPR Roles and Responsibilities · Personal Data Analysis Procedure
Art 27	Representative in the Union	Scope and accountability	To assign	GDPR Readiness Statement · General Privacy Policy
Art 5(1)(c)	Data minimisation	Principles and lawful basis	IT Manager 29 Oct 2026	Personal Data Analysis Form · Personal Data - Initial Questionnaire

Art 7	Conditions for consent	Principles and lawful basis	To assign	Procedure for Consent Management · Consent Request Form +1 more
Art 9	Special categories of personal data	Principles and lawful basis	Operations Manager 10 Dec 2026	Procedure for Processing of Special Categories of Personal Data · Personal Data Analysis Form
Art 12(1)	Transparent communication	Transparency and notices	HR Manager 24 Dec 2026	Privacy Notice Procedure · General Privacy Policy +1 more
Art 13(1)	Information where data is collected from the individual	Transparency and notices	To assign	Privacy Notice Planning Form - Data Subject · General Privacy Policy +1 more
Art 14(3)	Timing of notice for indirect collection	Transparency and notices	Risk Manager	Privacy Notice Procedure · Privacy Notice Planning Form - Other Source
Art 17(2)	Erasure by downstream recipients	Data subject rights	To assign	Data Subject Request Procedure · Records of Processing Activities
Art 19	Notification to recipients	Data subject rights	HR Manager 4 Feb 2027	Data Subject Request Procedure · Records of Processing Activities
Art 28(3)	Processor contract terms	Processors and third parties	Risk Manager 24 Dec 2026	Data Processing Agreement · GDPR Controller-Processor Agreement Policy +1 more
Art 29	Processing on documented instructions	Processors and third parties	To assign	Data Processing Agreement · GDPR Letter to Processors
Art 25(2)	Data protection by default	Data protection by design and security	Operations Manager 7 Jan 2027	Guidance for Data Protection by Design and Default · Data Protection Policy
Art 32(4)	Staff acting under authority	Data protection by design and security	To assign	Acceptable Use Policy · Information Security Policy
Art 34(1)	Communicating to affected individuals	Personal data breaches	To assign	Breach Notification Letter to Data Subjects · Personal Data Breach Notification Procedure
Art 38(3)	DPO independence and conflicts	Data protection officer	Operations Manager 29 Oct 2026	GDPR Roles and Responsibilities
Art 46(TIA)	Transfer impact assessment	International transfers	HR Manager	Procedure for International Transfers of Personal Data · Risk Register
Art 48	Third country authority requests	International transfers	HR Manager 21 Jan 2027	Procedure for International Transfers of Personal Data · Guidance on Engagement with Data Protection Authorities
Art 49	Derogations	International transfers	To assign	Procedure for International Transfers of Personal Data

LOW Implemented, not evidenced · 14

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
Art 24(2)	Data protection policies	Scope and accountability	To assign	Data Protection Policy · Internal Data Protection Policy +1 more
Art 5(1)(e)	Storage limitation	Principles and lawful basis	To assign	Retention Policy · Records Retention and Protection Policy
Art 10	Criminal conviction data	Principles and lawful basis	To assign	Procedure for Processing of Special Categories of Personal Data
Art 14(1)	Information where data is not obtained from the individual	Transparency and notices	To assign	Privacy Notice Planning Form - Other Source · Privacy Notice Procedure
Art 14(5)	Exemptions from indirect notice	Transparency and notices	To assign	Privacy Notice Procedure · Compliance Evidence
Art 18	Right to restriction of processing	Data subject rights	To assign	Procedure for Managing Data Subject Rights · Data Subject Request Procedure
Art 30(4)	Making the record available	Records of processing	To assign	Records of Processing Activities · GDPR Documentation Log
Art 28(2)	Sub-processors	Processors and third parties	To assign	Sub-Processor Agreement · GDPR Controller-Processor Agreement Policy
Art 32(1)(a)	Pseudonymisation and encryption	Data protection by design and security	To assign	Cryptographic Policy · Information Security Policy
Art 32(1)(d)	Testing and evaluating measures	Data protection by design and security	To assign	Information Security Policy · Risk Register
Art 34(3)	Exemptions from individual communication	Personal data breaches	To assign	Personal Data Breach Notification Procedure · Personal Data Breach Register
Art 35(1)	When a DPIA is required	DPIA and prior consultation	To assign	Data Protection Impact Assessment Process · Data Protection Impact Assessment Questionnaire
Art 36	Prior consultation	DPIA and prior consultation	To assign	Guidance on Engagement with Data Protection Authorities · Data Protection Impact Assessment Report
Art 40	Codes of conduct	Governance and assurance	To assign	Compliance Evidence · GDPR Documentation Log

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com