SAMPLE REPORT - FICTIONAL ORGANISATION

GOVERNANCE DOCS

UK GDPR and the Data Protection Act 2018

Gap Assessment Report

UK GDPR, the Data Protection Act 2018 and PECR, as amended by the Data (Use and Access) Act 2025

Thameside Lettings (sample)

Personal data of landlords, tenants, applicants and staff across 14 UK branch offices and the lettings platform.

ASSESSED	25 September 2026
EDITION	UK GDPR and DPA 2018 as amended by the Data (Use and Access) Act 2025
IN SCOPE	54 requirements, 54 applicable
PROFILE	Professional services · 50 to 249 people · Information Commission
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 Thameside Lettings (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Thameside Lettings (sample) stands against UK GDPR

OVERALL READINESS

61.1%

Level 2 · Developing

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

Initial | **Developing** | Established | Audit-ready

APPLICABLE	EVIDENCED	OPEN GAPS	HIGH PRIORITY
54	14	40	12

STATUS OF EVERY REQUIREMENT

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

GAPS WITH AN OWNER	WITH A TARGET DATE	NOT ANSWERED
19 of 40	7 of 40	0

WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 61.1% against UK GDPR across 54 applicable controls. 14 of them are implemented and evidenced.
- Most open gaps: Lawful basis and principles, with 10 at 35%. Strongest area: Governance and assurance at 92%.
- 13 controls are operating but not evidenced. Collecting their records alone lifts the score to 67.1% (+6.0 points), the cheapest gain available.
- 12 gaps are high priority (not started or only planned); 5 of them are in Lawful basis and principles.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	**Put an owner and date against the 5 high-priority gaps in Lawful basis and principles**	HR Manager	Lawful Basis Assessment Procedure
2	MEDIUM	**Adopt and tailor the Legal Crosswalk Workbook (Excel), which closes 3 open gaps**	To assign	Legal Crosswalk Workbook (Excel)
3	LOW	**Evidence the 13 controls that already operate (+6.0 points)**	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

At 61.1% readiness, the organization should immediately establish lawful bases and policy documents to resolve critical operational gaps.

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 shows an overall readiness score of 61.1% at the Developing level. Although our governance structures score 91.7%, we face exposure from 40 open gaps, including 12 high-priority items in lawful processing bases, international data transfers, and vendor due diligence. Operating without formal documentation creates operational vulnerability under review by the Information Commission. We need executive support to assign owners to all open gaps and allocate time for teams to formalize undocumented operating practices.

WHERE YOU STAND

Your self-assessment shows an overall score of 61.1%, placing the organization at readiness level 2 of 4, described as Developing. Out of 54 applicable requirements, you have 40 open gaps, including 12 high-priority gaps. While 14 requirements are implemented and evidenced, 15 are partially implemented and 13 are implemented without formal evidence. Control areas such as Governance and assurance scored 91.7%, but areas like International transfers scored 33.3% and Lawful basis and principles scored 35%. Currently, 19 gaps have an assigned owner and 7 have a target date.

WHAT IT MEANS FOR THE ORGANIZATION

The pattern indicates that foundational oversight exists, but operational execution and formal documentation lag behind. Having 13 requirements running without evidence means current practices cannot be verified during an inquiry. Furthermore, having 10 open gaps in Lawful basis and principles creates operational vulnerabilities across client services. Gaps in cross-border transfers and third-party vendor arrangements also matter to the expectations of the Information Commission. Addressing unevidenced work and unassigned gaps will improve accountability across your 50 to 249 people workforce.

WHERE TO FOCUS FIRST

You should focus first on resolving the 12 high-priority gaps that lack operational foundations. Immediate effort belongs on establishing lawful bases for processing, creating an appropriate policy document, and managing legitimate interests assessments. Concurrently, you should assemble documentation for the 13 practices that are already active to raise your readiness score from 61.1% to 67.1%. Assigning owners and realistic completion targets to the remaining 21 unassigned gaps will ensure accountability across all operational teams without delaying active business operations.

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1	**Establish lawful bases and special category policies** Art 6(1) Lawful basis for each purpose · DPA Sch 1 Pt 4 Appropriate policy document	Processing personal data without documented lawful grounds undermines operational legitimacy. This exposes business activities to regulatory scrutiny from the Information Commission.	Draft the lawful basis register for all current processing purposes across your business operations.	**Lawful Basis Register (Excel)** UK GDPR Toolkit – 90 UK Data Protection Templates (DUAA 2025)	30 DAYS
2	**Document cross-border transfer mechanisms and joint controller agreements** Art 46(1A) Transfer mechanisms and the data protection test · Art 26 Joint controllers	Unregulated international data flows and joint processing arrangements create material cross-border exposure. Addressing these ensures third-party operations remain defensible.	Complete transfer risk assessments for third-party service destinations currently handling client data.	**Transfer Risk Assessment Template** UK GDPR Toolkit – 90 UK Data Protection Templates (DUAA 2025)	60 DAYS
3	**Standardize legitimate interests assessments and consent collection** Art 6(1)(f) Legitimate interests assessments · Art 7 Consent	Unverified reliance on legitimate interests or improper consent forms compromises customer intake. Formal records substantiate your operational reliance on these legal justifications.	Apply the assessment template to ongoing commercial marketing and client processing activities.	**Legitimate Interests Assessment Template** UK GDPR Toolkit – 90 UK Data Protection Templates (DUAA 2025)	60 DAYS
4	**Implement processor due diligence and breach recording** Art 28(1) Processor due diligence · Art 33(5) Breach register	Inadequate supplier vetting and missing incident logs increase third-party delivery risks. Documented records are necessary to satisfy supervisory expectations during reviews.	Circulate the processor due diligence checklist to key professional services vendors.	**Processor Due Diligence Checklist** UK GDPR Toolkit – 90 UK Data Protection Templates (DUAA 2025)	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Populate the lawful basis register across all active business departments.
- Draft the appropriate policy document for handling special category data.
- Gather evidence for the 13 implemented but unevidenced requirements.
- Assign designated owners and target dates to all unowned gaps.

DAYS 31 TO 60

- Conduct transfer risk assessments for all international vendor data transfers.
- Execute formal joint controller arrangements with identified operational partners.
- Standardize legitimate interests assessments using the approved evaluation template.
- Update customer and employee privacy notices with accurate processing terms.

DAYS 61 TO 90

- Distribute the processor due diligence checklist to all existing data processors.
- Operationalize the personal data breach register across technical and administrative teams.
- Establish screening procedures for marketing calls under direct marketing standards.
- Review rights request handling processes to ensure statutory deadlines are recorded.

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	1 · 2 · 2	55%	1 · 2 · 2
Lawful basis and principles	3 · 2 · 3 · 2	35%	5 · 3 · 2
Transparency and notices	1 · 1 · 2	81%	0 · 1 · 1
Data subject rights	1 · 1 · 2 · 2	71%	1 · 1 · 2
Automated decisions and complaints	2 · 1	58%	0 · 2 · 1
Records and DPIA	3 · 1	56%	0 · 3 · 1
Processors and data sharing	1 · 1 · 1 · 1	50%	2 · 0 · 1
Security and breaches	1 · 4	85%	1 · 0 · 0
International transfers	1 · 2	33%	1 · 2 · 0
Marketing, cookies and PECR	1 · 3	63%	1 · 0 · 3
Governance and assurance	1 · 5	92%	0 · 1 · 0

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

WHERE THE NEXT POINTS COME FROM

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

Today	61.1%	
Evidence what already runs 13 requirements	67.1%	+6.0
Finish what is partly in place 15 requirements	81.0%	+13.9
Implement what is planned 7 requirements	90.7%	+9.7
Start what has not begun 5 requirements	100.0%	+9.3

DOCUMENTS THAT CLOSE THE MOST GAPS

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

Legal Crosswalk Workbook (Excel)	3
UK Data Protection Policy	3
Lawful Basis Register (Excel)	3
Lawful Basis Assessment Procedure	2
Special Category and Criminal Offence Data Policy	2
Consent Management Procedure and Consent Form	2

All of these are in the UK GDPR Toolkit (90 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 · 5**

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 6(1)	Lawful basis for each purpose	Lawful basis and principles	HR Manager	Lawful Basis Assessment Procedure · Lawful Basis Register (Excel)
DPA Sch 1 Pt 4	Appropriate policy document	Lawful basis and principles	Compliance Lead 29 Oct 2026	Appropriate Policy Document · Special Category and Criminal Offence Data Policy
Art 8	Children's data	Lawful basis and principles	Operations Manager	Children's Data Procedure · Consent Management Procedure and Consent Form
Art 26	Joint controllers	Processors and data sharing	Compliance Lead 24 Dec 2026	Joint Controller Arrangement
Art 46(1A)	Transfer mechanisms and the data protection test	International transfers	Operations Manager	Transfer Risk Assessment Template · IDTA Completion Guide +1 more

HIGH **Planned · 7**

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

Ref	Requirement	Area	Owner · target	Closes it
DUAA 2025	The 2025 Act changes	Scope and accountability	Operations Manager	DUAA 2025 Change Register (Excel) · Legal Crosswalk Workbook (Excel)
Art 6(1)(f)	Legitimate interests assessments	Lawful basis and principles	Risk Manager 24 Dec 2026	Legitimate Interests Assessment Template · Lawful Basis Assessment Procedure
Art 7	Consent	Lawful basis and principles	HR Manager	Consent Management Procedure and Consent Form
Arts 16-18	Rectification, erasure and restriction	Data subject rights	To assign	Rectification, Erasure and Restriction Procedure · Rights Request Register (Excel)
Art 28(1)	Processor due diligence	Processors and data sharing	IT Manager	Processor Due Diligence Checklist · Sub-Processor Register (Excel)

Art 33(5)	Breach register	Security and breaches	Risk Manager 7 Jan 2027	Personal Data Breach Register (Excel)
PECR r21	Marketing calls	Marketing, cookies and PECR	Operations Manager 21 Jan 2027	TPS and CTPS Screening Procedure

MEDIUM **Partially implemented · 15**

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

Ref	Requirement	Area	Owner · target	Closes it
Art 27	UK representative	Scope and accountability	To assign	Data Protection Roles and RACI Matrix · UK Data Protection Policy
Art 5(2)	Accountability	Scope and accountability	To assign	Accountability Framework and Compliance Calendar · UK Data Protection Policy
Art 5(1)	Data protection principles	Lawful basis and principles	HR Manager	UK Data Protection Policy · Legal Crosswalk Workbook (Excel)
Art 8A	Purpose compatibility	Lawful basis and principles	HR Manager 21 Jan 2027	Purpose Compatibility Assessment Template
Art 5(1)(e)	Retention	Lawful basis and principles	Operations Manager	Records Retention Schedule (Excel) · HR Data Retention Schedule (Excel)
Art 13	Privacy notices at collection	Transparency and notices	HR Manager	Privacy Notice Procedure · Customer Privacy Notice +3 more
Art 12A	Time limits for rights requests	Data subject rights	Operations Manager 10 Dec 2026	Data Subject Access Request Procedure · DSAR Log (Excel) +1 more
Arts 22B-22C	Automated decision safeguards	Automated decisions and complaints	To assign	Automated Decision-Making Procedure
DPA s164A	Complaints procedure	Automated decisions and complaints	To assign	Data Protection Complaints Procedure · Complaints Log (Excel) +1 more
Art 30	Records of processing	Records and DPIA	HR Manager	Records of Processing Procedure · Records of Processing Register (Excel)
Art 36	Prior consultation	Records and DPIA	HR Manager	Prior Consultation Procedure · DPIA Template
Art 25	Data protection by design and default	Records and DPIA	To assign	Data Protection by Design and Default Procedure
Art 44	Mapping transfers	International transfers	To assign	International Transfers Procedure · Transfer Register (Excel)

Art 45A	Adequate destinations	International transfers	To assign	Adequacy and Transfer Mechanisms Reference (Excel) · Transfer Register (Excel)
REG	Dealing with the regulator	Governance and assurance	Compliance Lead	ICO Engagement and Regulatory Notices Procedure

LOW **Implemented, not evidenced · 13**

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 3	Territorial scope	Scope and accountability	To assign	UK GDPR Toolkit Implementation Guide · Legal Crosswalk Workbook (Excel)
DP Charges Regs	Data protection fee	Scope and accountability	To assign	ICO Fee Registration Procedure
Art 6(1)(ea)	Recognised legitimate interests	Lawful basis and principles	To assign	Recognised Legitimate Interests Procedure · Lawful Basis Register (Excel)
Art 9	Special category data	Lawful basis and principles	To assign	Special Category and Criminal Offence Data Policy · Lawful Basis Register (Excel)
Art 14	Data obtained from others	Transparency and notices	To assign	Privacy Notice Procedure · Supplier and Business Contact Privacy Notice
Art 15(1A)	Reasonable and proportionate searches	Data subject rights	To assign	Data Subject Access Request Procedure · DSAR Log (Excel)
DPA Sch 2	Exemptions	Data subject rights	To assign	Schedule 2 Exemptions Guide · Rights Request Register (Excel)
Art 22A	Identifying automated decisions	Automated decisions and complaints	To assign	Automated Decision-Making Procedure · Records of Processing Register (Excel)
Art 35	Data protection impact assessments	Records and DPIA	To assign	DPIA Procedure · DPIA Screening Questionnaire +2 more
Art 28	Processor contracts	Processors and data sharing	To assign	Data Processing Agreement (UK GDPR Article 28) · Processor Clause Guide
PECR r22	Electronic marketing consent	Marketing, cookies and PECR	To assign	Direct Marketing Policy · PECR Compliance Procedure +1 more

PECR r6	Cookies and similar technologies	Marketing, cookies and PECR	To assign	Cookie Policy and Consent Procedure · PECR Compliance Procedure
PECR r5A	PECR breaches for service providers	Marketing, cookies and PECR	To assign	PECR Breach Notification Note for Service Providers

A · ABOUT THIS REPORT

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