GDPR for Mid-Market Companies: What Leadership Needs to Know

A practical compliance reference for finance and compliance leaders at companies processing personal data in Europe

fortifai

What GDPR Is and Why It Still Demands Attention

The General Data Protection Regulation has been in force since May 25, 2018. Most mid-market companies did something about it then — a privacy policy update, a consent refresh, a data mapping exercise. Many assumed that was sufficient. **It was not — and enforcement data is making that clear.**

Fines against mid-market companies have increased significantly since 2022. Datatilsynet and its European counterparts are conducting proactive audits, investigating individual complaints that reveal systemic gaps, and issuing proportionate fines to companies of all sizes.

> The fundamental issue is that GDPR is not a one-time compliance project. It is an ongoing operational obligation that requires documented decisions, maintained records, and working governance processes — year after year, as processing activities change and new tools are adopted.

Three things make GDPR compliance harder in 2024 than it was in 2018:

Processing has expanded

The same company that processed personal data through a CRM and email list in 2018 now processes it through AI tools, marketing automation platforms, analytics systems, cloud infrastructure across multiple jurisdictions, and dozens of SaaS integrations. The data map from 2018 is not accurate anymore.

Enforcement has matured

Supervisory authorities have built capacity and are using it. The era of GDPR being primarily a large-company problem is over.

Regulatory interpretation has evolved

Court decisions, EDPB guidance, and national authority decisions since 2018 have clarified obligations in ways that have raised the bar on legitimate interests assessments, international data transfers, data subject rights responses, and processor due diligence.

Key Definitions Leadership Needs to Know

GDPR uses specific terminology that carries legal weight. These are the definitions most relevant to governance decisions at management level:

Data Controller	The organisation that determines the purposes and means of processing personal data — your company, in most cases
Data Processor	A third party that processes personal data on your behalf — your SaaS vendors, cloud providers, analytics tools
Personal Data	Any information relating to an identified or identifiable natural person — broader than most companies realise, includes IP addresses, device IDs, and behavioural data
Lawful Basis	The legal justification for processing personal data — one of six bases must apply to every processing activity
Legitimate Interests	One lawful basis — requires a three-part documented assessment balancing your interests against the rights of data subjects
Data Processing Agreement	A mandatory contract between controller and processor — required for every third-party tool that processes personal data on your behalf
Records of Processing Activities	A documented inventory of all processing activities — required under Article 30 for companies with 250+ employees and recommended for all others
Data Protection Impact Assessment	A structured risk assessment required before high-risk processing — includes AI processing, large-scale profiling, and systematic monitoring
Data Subject Rights	Rights held by individuals whose data you process — access, erasure, rectification, portability, restriction, objection

Who GDPR Applies To

GDPR applies to any organisation that processes personal data of individuals in the EU or EEA — **regardless of where the organisation is headquartered.** Norwegian companies are subject to GDPR through the EEA agreement. Datatilsynet is Norway's supervisory authority and has full enforcement powers including fines, corrective orders, and publication of enforcement decisions.

Foreign companies selling to Norwegian or EU customers, employing people in Norway or the EU, or using cookies and analytics on websites accessed by EU and EEA users are subject to GDPR regardless of where they are based.

The DPO Requirement

Companies must appoint a Data Protection Officer if they conduct large-scale systematic monitoring of individuals, process special category data on a large scale, or are a public authority.

Many mid-market companies in health tech, HR tech, fintech, and adtech fall within scope.

Best Practice — Even Without a Formal DPO

Even where a formal DPO is not required, a named data protection contact with defined responsibilities is strong practice and expected by Datatilsynet.

- Health tech
- HR tech
- Fintech
- Adtech

What GDPR Requires From You as Leadership

GDPR's accountability principle — **Article 5(2)** — requires that controllers not only comply with GDPR but be able to demonstrate that they comply. This means documented decisions, named owners, and retrievable evidence at the management level.

What You're Signing or Owning	When	What Datatilsynet Checks
Lawful Basis Decisions	Before processing begins, reviewed when processing changes	Documented decision for each processing activity, named owner, rationale
Legitimate Interests Assessment	Before relying on LIA as lawful basis	Three-part test documented, signed off at appropriate level
Data Protection Impact Assessments	Before high-risk processing begins	Completed assessment, documented outcome, sign-off
Processor Agreement Approvals	Before sharing data with any processor	Signed DPA meeting Article 28 requirements, current SCCs for international transfers
Records of Processing Activities	Maintained continuously	Current, accurate ROPA covering all processing activities
Breach Notification Decision	Within 72 hours of becoming aware	Documented assessment of risk, notification decision, evidence of filing
Data Subject Rights Responses	Within one month of request	Response sent, documented, within statutory timeframe
Annual GDPR Governance Review	Annually minimum	Evidence of management-level review, decisions documented
Privacy Notice Updates	When processing activities change	Current notices reflecting actual processing, version history

The accountability principle is the most important concept for CFOs to internalise. GDPR does not just require you to comply — it requires you to be able to prove that you comply. A company that processes data lawfully but cannot produce documented evidence of its lawful basis decisions, LIA assessments, and processor agreements is non-compliant with the accountability principle regardless of the underlying compliance of its processing.

The breach notification obligation is the highest-risk area operationally. **72 hours from becoming aware of a breach is an extremely short window.** The clock starts when anyone in your organisation becomes aware — not when the IT team has completed their assessment. A breach response procedure that requires multiple sign-offs, legal review, and manual drafting will not meet the deadline consistently. This procedure must be built, tested, and owned by a named person before a breach occurs.

The Six Lawful Bases — A Leadership Reference

Every processing activity requires a lawful basis. This is the decision most organisations document poorly — either choosing a basis that does not actually apply, or failing to document the decision at all.

Lawful Basis	What It Covers	Most Common Mid-Market Use Cases
Contract	Processing necessary to perform a contract with the data subject	Customer service, order fulfilment, employee payroll
Legal obligation	Processing required by law	Tax records, employment records, regulatory reporting
Vital interests	Processing to protect life	Rare — emergency contact situations
Public task	Processing for a task in the public interest	Public sector and certain regulated entities only
Legitimate interests	Processing for your legitimate interests, balanced against data subject rights	B2B marketing, fraud prevention, network security, analytics
Consent	Freely given, specific, informed, unambiguous agreement	B2C marketing, non-essential cookies, research participation

Legitimate Interests — The Three-Part Test

Legitimate interests is the basis most mid-market companies rely on most broadly — and document least carefully. The three-part test requires:

1. A **purpose test** — is the purpose legitimate?
2. A **necessity test** — is processing necessary for that purpose?
3. A **balancing test** — do your interests override the data subject's rights and freedoms?

Each test must be documented. The balancing test in particular requires a named executive to make a judgment call and sign off on it. Most companies that rely on LIA have never produced this documentation.

Consent — Frequently Misused

Consent must be:

- **Freely given** — the data subject must have a genuine choice
- **Specific** — separate consent for each purpose
- **Unambiguous** — a clear affirmative action, not a pre-ticked box
- **As easy to withdraw as to give**

Many mid-market companies rely on consent for processing that does not actually meet these requirements, creating exposure they are not aware of.

High-Level Compliance Checklist:

Phase 1 — Data Mapping and ROPA

- Build or update Records of Processing Activities — every processing activity, lawful basis, data categories, retention period, processors involved, international transfers
- Map all personal data flows — where data enters, how it moves, where it goes, who can access it
- Identify all data processors — every SaaS tool, cloud service, and third party that processes personal data on your behalf
- Identify all international data transfers — data moving outside the EEA requires adequate safeguards
- Appoint named GDPR compliance owner — with executive sponsor at board level
- Assess DPO requirement — appoint or document why appointment is not required

Phase 2 — Lawful Basis and Documentation

- Review lawful basis decision for each processing activity in the ROPA
- Complete Legitimate Interests Assessments for all processing relying on LIA — three-part test, executive sign-off
- Review consent mechanisms — confirm consent is freely given, specific, informed, and unambiguous where relied upon
- Document lawful basis decisions with named owner and date for each processing activity
- Review and update all privacy notices to reflect current, accurate processing
- Build consent withdrawal mechanism for all consent-based processing

Phase 3 — Processor Agreement Audit

- Audit all third-party tools and services for personal data processing
- Confirm Data Processing Agreement in place for each processor — meeting Article 28 requirements
- Review international transfer mechanisms — confirm SCCs are current post-Schrems II for non-EEA processors
- Flag processors without adequate agreements — resolve or replace
- Build processor onboarding process — DPA required before any new processor is activated
- Schedule annual processor agreement review

High-Level Compliance Checklist:

Phase 4 — Data Subject Rights Framework

- Build DSAR response procedure — who receives, who coordinates, which systems are searched, who signs off
- Map where personal data sits across all systems — essential for responding to access and erasure requests
- Build erasure procedure — how data is deleted across all systems and processors when requested
- Build portability procedure — how data is exported in machine-readable format on request
- Set up tracking for rights requests — receipt date, response deadline, status, outcome
- Test the procedure — run a simulated DSAR end to end

Phase 5 — Breach Response Framework

- Define what constitutes a personal data breach for your organisation
- Build breach assessment procedure — who decides whether to notify, on what criteria, within what timeframe
- Identify Datatilsynet notification process and contact details
- Build 72-hour notification template — pre-populated with standard information required
- Define data subject notification procedure for high-risk breaches
- Test the procedure — run a simulated breach response exercise
- Named executive owner for breach notification decisions

Phase 6 — High-Risk Processing and DPIAs

- Identify all processing activities that may require a DPIA — AI processing, large-scale profiling, systematic monitoring, special category data
- Complete DPIAs for identified high-risk processing activities
- Executive sign-off on DPIA outcomes and residual risk decisions
- Consult Datatilsynet where DPIA identifies high residual risk that cannot be mitigated

Phase 7 — Ongoing Compliance

- Annual GDPR governance review — management-level review of processing activities, incidents, rights requests, and processor relationships
- Annual ROPA update — review and update as processing activities change
- Annual processor agreement review — confirm DPAs are current and processors remain adequate
- Annual privacy notice review — confirm notices reflect current processing
- Annual LIA review — reassess legitimate interests decisions as processing context changes
- Monitor EDPB guidance and Datatilsynet enforcement decisions for updates to compliance expectations

The Five Most Common GDPR Gaps

These are the findings that appear most consistently in Datatilsynet audits and investigations of mid-market companies:

1

ROPA is out of date or does not exist

The Records of Processing Activities is the foundation of demonstrable GDPR compliance. An out-of-date ROPA that does not reflect current processing — including new SaaS tools, AI integrations, and changed business processes — is an immediate finding. Article 30 requires it to be maintained continuously, not created once.

2

No DPA for key processors

Marketing automation, CRM platforms, HR systems, analytics tools, and AI services all process personal data on your behalf. Each requires a Data Processing Agreement meeting Article 28 requirements. Many mid-market companies have signed DPAs for their largest processors but have accumulated dozens of tools without proper agreements. International transfers to non-EEA processors additionally require current Standard Contractual Clauses.

3

LIA not documented

Legitimate interests is a valid and useful lawful basis — but only if the three-part assessment is documented and signed off. A company that has been relying on LIA for B2B marketing or analytics without a documented assessment has no evidence of compliance if challenged.

4

DSAR procedure is ad hoc

Data subject access requests arrive without warning and have a one-month response deadline. Companies that respond ad hoc — searching manually across systems, coordinating informally across teams, drafting responses from scratch each time — consistently miss deadlines or produce incomplete responses. One incomplete DSAR response is the most common trigger for an individual complaint to Datatilsynet.

5

Breach response is not tested

The 72-hour notification requirement is the GDPR obligation with the most immediate operational consequences. Companies that have a breach response policy but have never tested it discover under pressure that the procedure does not work — key decision-makers are unavailable, systems cannot be queried quickly enough, and the Datatilsynet notification template is being drafted for the first time during an active incident.

Manual vs. Automated: What Good Looks Like

GDPR Requires	Manual Reality	With Governance Automation
Current ROPA covering all processing	Spreadsheet last updated at implementation	Live register updated when processing changes, with review triggers
Documented LIA for each legitimate interests reliance	Decision made once verbally, never written down	Three-part test documented, signed off, version-controlled
DPA in place for every processor	Large vendors covered, smaller tools overlooked	Processor inventory with DPA status tracked and gaps flagged
DSAR response within one month	Ad hoc process, inconsistent quality, deadline risk	Structured workflow with receipt tracking, system searches coordinated, sign-off trail
72-hour breach notification	Procedure exists on paper, never tested	Pre-built assessment framework, notification template, named decision-maker ready
Annual governance review with documented outputs	Meeting happened, no documented outcome	Structured review with timestamped sign-off and action log

GDPR is continuous. Processing activities change every time a new tool is adopted. A processor agreement becomes outdated when a vendor updates its sub-processor list. A privacy notice becomes inaccurate when a new analytics platform is added. Companies that treat GDPR as infrastructure — maintained continuously rather than revisited annually — are the ones that handle Datatilsynet scrutiny without scrambling.

The Connection to ISO 27001, NIS2, and EU AI Act

GDPR does not exist in isolation. For mid-market companies managing multiple compliance obligations, the overlap with other frameworks is significant:

GDPR and ISO 27001

Information security management and data protection share processor due diligence, incident response, access control, and management review workflows. The evidence base overlaps directly. Companies certified under ISO 27001 have a strong foundation for GDPR accountability.

GDPR and NIS2

Incident reporting obligations overlap. A cybersecurity incident that involves personal data triggers both NIS2 reporting to the national competent authority and GDPR breach notification to Datatilsynet. A single incident response procedure that satisfies both timelines is more efficient than two separate processes.

GDPR and EU AI Act

AI systems processing personal data require both GDPR-compliant data governance and EU AI Act compliance. The Data Protection Impact Assessment under GDPR and the Fundamental Rights Impact Assessment under the EU AI Act address overlapping questions. A unified workflow handles both.

GDPR and Åpenhetsloven

Supply chain due diligence under Åpenhetsloven and processor due diligence under GDPR both require structured supplier assessments, documented findings, and ongoing review. The governance infrastructure is shared.

For mid-market companies managing all of these — and increasingly that is most companies above a certain size — Fortifai's governance platform handles them from a single evidence base, which means each additional framework costs a fraction of the first.

What the Penalties Look Like

Less Severe Violations — Article 83.4

Includes ROPA failures, processor agreement failures, DPO obligations

€10 million or 2% of global annual turnover — whichever is higher

More Severe Violations — Article 83.5

Includes unlawful processing, data subject rights violations, international transfer failures

€20 million or 4% of global annual turnover — whichever is higher

Datatilsynet Enforcement Examples in Norway

Company	Fine	Reason
Grindr	NOK 65 million	Unlawful sharing of personal data with advertisers
Disqus	NOK 25 million	Processing without valid legal basis
Bergen municipality	NOK 5 million	Inadequate access controls to student records
Ferde	NOK 5 million	Unlawful processing of location data

The pattern in mid-market enforcement is consistent: companies that processed data without adequate lawful basis documentation, that lacked processor agreements for key vendors, or that could not produce evidence of the decisions they claim to have made.

How Fortifai Supports This

Fortifai is governance workflow infrastructure built for growing and mid-market companies. The platform automates the three workflows GDPR requires:

Sign-off Routing and Tracking

For lawful basis decisions, LIA sign-offs, DPIA approvals, and breach notification decisions

Disclosure Document Management

For privacy notices, the ROPA, DPAs, and Datatilsynet correspondence

Information Request Handling

For DSARs, processor questionnaires, and regulatory evidence requests — pre-configured for GDPR with templates ready on day one

The same platform supports **ISO 27001, NIS2, EU AI Act, ISO 42001, Åpenhetsloven,** and other frameworks simultaneously. For mid-market companies managing multiple compliance obligations, the governance workflows overlap significantly and the evidence base is shared — meaning each additional framework costs a fraction of starting from scratch.

> Used by teams at **Cognite, Aker BioMarine, and Telenor.**

Book a 30-minute walkthrough at fortifai.co

fortifai