GDPRGard • Research

European GDPR Compliance Report 2026

A research synthesis of published GDPR compliance data across European organizations

11 compliance dimensions analyzed — RoPA, DPIA, DPA vendor contracts, cookie consent, DSAR readiness, breach preparedness, AI governance, third-party SaaS risk, international transfers, DPO appointment, and employee training — drawn from IAPP-EY, DLA Piper, Cisco, Ponemon, EDPB, ICO, CNIL, Hiscox, EY Law, SecurityScorecard, DIGITALEUROPE, and peer-reviewed academic research.

Published August 2026 • gdprgard.eu

Independent research synthesis — not a GDPRGard-commissioned primary survey. See Methodology & Sources, p.3, for full sourcing.

Contents

Methodology & Sources	3
Key Findings at a Glance	4
01 Records of Processing Activities (RoPA)	5
02 Data Protection Impact Assessments (DPIA)	5
03 Data Processing Agreements (DPA) with Vendors	5
04 Cookie Consent & Website Compliance	6
05 DSAR Readiness	7
06 Data Breach Preparedness	7
07 AI Usage & AI Governance	8
08 Third-Party & SaaS Vendor Risk	8
09 International Data Transfers	9
10 DPO Appointment	9
11 Employee GDPR Training	9
Cross-Cutting Themes & Conclusion	11
Recommendations for Businesses	11
Full Source List	12

Methodology & Sources

This report is a **research synthesis**, not a newly-commissioned survey. GDPRGard did not field a primary questionnaire to 500 businesses for this edition. Instead, every statistic below is drawn from an existing, named, publicly available study, regulator report, or enforcement dataset, cited at the point of use and listed in full in the Source List (p.16). Collectively these sources represent survey and audit coverage well beyond 500 organizations — including a 254,148-website academic compliance sweep, a 17,490-stakeholder EDPB coordinated enforcement action, and multi-thousand-respondent industry benchmarks from IAPP-EY, Cisco, Ponemon, and EY Law — spanning 2018 through early 2026.

Where a genuinely current (2023–2026), EU-specific figure could not be located for a given dimension, we say so explicitly in a flagged “Data Gap” note rather than estimate a number. Several figures are the most recent available but predate 2023, or are drawn from global/US-UK samples used as a labelled proxy where no EU-specific equivalent exists — both are marked inline. Readers should treat every statistic as attributable to its named source, not to GDPRGard.

Source families used: IAPP / IAPP-EY Privacy Governance & AI Governance Reports; DLA Piper GDPR Fines and Data Breach Survey (2026); Cisco Data Privacy Benchmark Study; Ponemon Institute and Ponemon-Sullivan Privacy Report third-party risk studies; EDPB and EDPS coordinated enforcement and DPIA survey reports; UK ICO and French CNIL enforcement data; Hiscox Cyber Readiness Report; EY Law DSAR Survey; SecurityScorecard Global Third-Party Breach Report; DIGITALEUROPE Schrems II Impact Survey; and a peer-reviewed ACM CHI 2025 academic study of cookie banners across 31 EU/EEA countries.

Key Findings at a Glance

Headline figures for each of the eleven dimensions covered in this report. Full context, sample details, and citations for every number appear in the corresponding section.

RoPA	~34% reported no RoPA / didn't know (2018 baseline)
DPIA	~40% had never conducted a DPIA (2018 baseline)
DPA / Vendor Contracts	Only 36% vet all vendors before data-sharing (2022)
Cookie Compliance	Only 15% of consent banners are minimally compliant (2025)
DSAR Readiness	51% of firms received complaints about DSAR handling (2023)
Breach Preparedness	443 breach notifications/day across Europe, +22% YoY (2026)
AI Governance	Up to 48-pt gap between AI use and formal AI governance (2024)
Third-Party / SaaS Risk	Only 36% of vendors in a portfolio get a risk assessment (2026)
International Transfers	85% of EU firms use SCCs; only 70% among SMEs (2020 baseline)
DPO Appointment	~70% of European orgs have ≥1 DPO, vs. 40% in North America (2024)
Employee Training	No current EU-specific figure located — flagged data gap

01 Records of Processing Activities (RoPA)

~34%

of GDPR-subject organizations had prepared no RoPA, or didn't know if they had one

IAPP-EY Daily Dashboard Survey, 2018, n=410

25%

had prepared only 1–5 RoPA reports in total since GDPR took effect

IAPP-EY Daily Dashboard Survey, 2018, n=410

Article 30 requires most organizations processing personal data to maintain a Record of Processing Activities. The most reliable business-wide figures available come from IAPP's original post-GDPR baseline survey: roughly a third of subject organizations had no RoPA at all in the law's first year, and a further quarter had built only a handful of records rather than a comprehensive one.

Enforcement-side evidence suggests the underlying problem has not disappeared: the EDPB's 2023 Coordinated Enforcement Action on cloud services in the public sector examined RoPA completeness as one of its checks, though we could not independently verify a specific current percentage from the primary EDPB report against secondary citations (see Data Gap below).

■ *DATA GAP — No current (2023–2026), EU-wide, business-focused RoPA completion rate from DLA Piper, Cisco, TrustArc, or OneTrust could be verified in this research pass. A widely circulated "37% of public bodies" figure attributed to the EDPB could not be confirmed against the primary source and should not be cited without independent verification.*

02 Data Protection Impact Assessments (DPIA)

~40%

of GDPR-subject organizations had never conducted a single DPIA

IAPP-EY Daily Dashboard Survey, 2018, n=410

Article 35 requires a DPIA before processing likely to result in high risk to individuals — large-scale monitoring, special-category data, or systematic profiling among the trigger conditions. In IAPP's 2018 baseline, 60% of subject organizations had completed at least one DPIA, implying roughly 40% had not, and most that had done any had completed fewer than five in total.

The EDPS's 2024 DPIA Survey Report (published September 2025) is the most recent dedicated study on this topic, but its scope is EU institutions, bodies, offices and agencies rather than private-sector businesses, and specific percentages could not be extracted from the available report excerpt.

■ *DATA GAP — No current, business-wide, EU-specific DPIA non-compliance percentage was located for 2023–2026. Cisco's 2025 Data Privacy Benchmark and TrustArc's 2025 Global Benchmarks Report (n=1,775) likely contain a usable figure but it did not surface in available excerpts.*

03 Data Processing Agreements (DPA) with Vendors

36%

of organizations evaluate the security and privacy practices of ALL vendors before starting a data-sharing relationship

Ponemon Institute, 2022 Data Risk in the Third-Party Ecosystem Study, n=1,162, N. America + W. Europe

Article 28 requires a written agreement whenever a processor handles personal data on a controller's behalf. Direct EU-specific DPA-execution-rate data proved difficult to source, but Ponemon's third-party risk research — covering North America and Western Europe — offers the closest reliable proxy: fewer than four in ten organizations evaluate every vendor's security and privacy practices before a data-sharing relationship begins, implying a majority sign agreements, or begin sharing data, without full due diligence on the counterparty.

This finding is consistent with the broader third-party risk picture in Section 08: vendor oversight gaps and DPA gaps tend to travel together, since both stem from immature vendor-onboarding processes.

■ *DATA GAP — Figures such as "54% of businesses do not vet vendors properly" circulate in secondary blog sources attributed to Ponemon/Prevalent but could not be traced to a specific, dated primary report — excluded from this report as unverified. No EU-specific, Article-28-focused DPA execution-rate survey was located.*

04 Cookie Consent & Website Compliance

15%

of consent interfaces are minimally GDPR-compliant (equal-prominence accept/reject, nothing pre-checked)

Nouwens et al., ACM CHI 2025, n=254,148 sites, 31 EU/EEA countries

67%

of the UK's top 200 websites were flagged non-compliant in a regulator sweep

UK ICO cookie compliance review, January 2025

Cookie and tracker consent remains the most heavily studied — and most consistently poor — compliance dimension in this report. The largest academic sweep to date, covering a quarter-million sites across every EU/EEA country, found only 15% of consent banners meet a minimal compliance bar; national compliance ranged from 28% in Spain down to 3% in Slovenia. A separate industry study (Privado.ai, November 2024) found 74% of top European websites do not honor opt-in consent as GDPR requires, and the ICO's own 2025 sweep of the UK's most-visited sites flagged two-thirds as non-compliant.

Enforcement has followed: the French CNIL alone issued 83 sanctions totalling roughly €486.8 million in 2025, with cookie and tracker violations forming the bulk of cases.

05 DSAR Readiness

60%
of financial-services firms reported a year-over-year increase in DSAR volume

EY Law, 2023 DSAR Survey, n=500+, global financial services

51%
received complaints about how a DSAR was handled

EY Law, 2023 DSAR Survey

88%
process DSARs entirely in-house, without dedicated tooling or outside support

EY Law, 2023 DSAR Survey

Articles 15–22 give individuals the right to access, correct, or erase their data, generally within one month. EY Law's 2023 survey of 500+ compliance professionals at financial-services firms — a sector with EU-wide reach — found rising request volumes outpacing internal process maturity: a third had received bulk requests, over half had fielded complaints about their handling of a request, and the large majority still manage the process manually rather than through dedicated DSAR software.

An older but frequently cited figure (Talend, via CIO Dive, 2019) found 58% of companies missed the then-required one-month deadline, an improvement from 70% the year before — useful as a directional trend line but too dated to state as a current rate.

■ *DATA GAP — No 2023–2026, EU-specific percentage for missed 30-day DSAR deadlines was located. DataGrail's 2025/2026 research confirms a 43% DSAR volume increase between 2023 and 2024 but does not publish a deadline-miss rate.*

06 Data Breach Preparedness

443
personal data breach notifications filed per day across Europe, up 22% year-over-year

DLA Piper GDPR Fines and Data Breach Survey, Jan 2026, 31 countries

59%
of businesses experienced a cyberattack in the past 12 months (Germany: 67%)

Hiscox Cyber Readiness Report 2025, multi-country SME/mid-market survey

DLA Piper's eighth annual survey, drawing on supervisory-authority data from 31 countries, found the daily average of breach notifications topped 400 for the first time since 2018, with cumulative GDPR fines since the regulation took effect reaching €7.1 billion — about €1.2 billion of that in 2025 alone. Hiscox's cross-country readiness survey found the majority of businesses had faced an attack in the prior year, with meaningful country variation (Germany 67%, Ireland 42%).

Both data points describe incident volume and exposure rather than internal preparedness directly. We were unable to locate a reliable EU-specific figure for the narrower question of how many organizations lack a formal incident-response plan or fail the 72-hour notification window — flagged below rather than estimated.

■ *DATA GAP — No EU-specific percentage for organizations lacking a formal incident-response plan, or failing the 72-hour breach notification window, was found in this research pass despite checking Hiscox, IBM Cost of a Data Breach, and ENISA Threat Landscape sources.*

07 AI Usage & AI Governance

77%

of organizations are actively working on AI governance (rises to ~90% among AI-users)

IAPP, AI Governance Profession Report 2025, global privacy professionals

74%→52%

of large organizations (>$60B revenue) use AI, but only 52% have an established AI governance function

IAPP-EY Privacy Governance Report 2024, global

As AI adoption accelerates alongside the EU AI Act's phased entry into force, governance is visibly lagging use. IAPP's global data — skewed toward privacy professionals, a reasonable proxy given IAPP's large EU membership base — shows that even among organizations already using AI, roughly one in ten to one in four have no formal governance effort underway. At the largest organizations, the gap between AI adoption (74%) and having an established governance function (52%) runs as high as 22 percentage points on the headline figures, and higher still once informal or partial governance efforts are excluded.

Cisco's 2025/2026 Data Privacy Benchmark studies confirm the direction — over 90% of companies report expanding privacy programs specifically to address AI — but did not yield a clean single "% without an AI policy" figure usable here.

■ *DATA GAP — No EU-specific percentage for businesses using AI without any GDPR/AI Act impact assessment was located; the figures above are global proxies, not EU-only measurements.*

08 Third-Party & SaaS Vendor Risk

52%

of organizations describe their third-party risk program as reactive, not proactive

Ponemon-Sullivan Privacy Report, State of Third-Party Risk Assessments, March 2026, n=1,465

36%

of vendors in an average 2,643-vendor portfolio actually receive a risk assessment

Ponemon-Sullivan Privacy Report, March 2026

35.5%

of all 2024 data breaches were linked to third-party access, up 6.5 points from 2023

SecurityScorecard, 2025 Global Third-Party Breach Report

The modern SaaS-heavy stack has pushed a growing share of data risk outside the organization's direct control. Ponemon-Sullivan's March 2026 survey of 1,465 IT and security practitioners (431 EMEA respondents) found just under a fifth of organizations consider their program "optimized," and barely a third of vendors in a typical portfolio are ever actually assessed — a coverage gap wide enough to leave most of the vendor estate effectively unmonitored.

SecurityScorecard's global breach dataset shows the consequence trending the wrong way: over a third of all 2024 breaches traced back to third-party access, a meaningful jump from the year before.

09 International Data Transfers

85%

of surveyed European companies use Standard Contractual Clauses (SCCs) for transfers

DIGITALEUROPE, Schrems II Impact Survey Report, 2020, n≈300 EU businesses

70%

SCC adoption specifically among SMEs, versus 85% across all surveyed firms

DIGITALEUROPE, Schrems II Impact Survey Report, 2020

Following the 2020 Schrems II ruling, DIGITALEUROPE's survey of roughly 300 EU businesses remains the most concrete EU-specific measurement of international-transfer-mechanism adoption available: the large majority of firms had adopted SCCs, though adoption ran meaningfully lower among SMEs than larger firms, consistent with the resource gap seen elsewhere in this report.

The transfer landscape has since shifted materially — the EU-US Data Privacy Framework took effect in 2023, and case law and EDPB guidance have continued to evolve — which makes a 2020 baseline dated context rather than a current compliance rate.

■ *DATA GAP — This is the most concrete EU transfer-mechanism-adoption survey located, but it predates the 2023 EU-US Data Privacy Framework. No 2023–2026 refresh of a comparably EU-specific transfer-compliance survey was found — a genuine gap in current published research, not an oversight.*

10 DPO Appointment

~70%

of European organizations have appointed at least one DPO (avg. 3–4 FTE DPOs)

IAPP-EY Privacy Governance Report 2024, global privacy professionals

~500,000

organizations are estimated to have registered DPOs across the EEA

IAPP research study, extrapolated from German federal/state DPA registration data

Where Article 37 requires a DPO — public authorities, large-scale monitoring, or large-scale special-category processing — European organizations appoint one at nearly double the rate of their North American counterparts (70% vs. 40%), and staff the role far more heavily once appointed (3–4 FTEs on average in Europe versus under one FTE in North America). IAPP's extrapolation from DPA registration data puts the EEA-wide DPO population at roughly 500,000 — about six times the organization's original 2017 estimate of the number that would be needed.

The EDPB's January 2024 Coordinated Enforcement Action surveyed 17,490 stakeholders (15,108 organizations and 2,382 DPOs) across 22 EEA supervisory authorities specifically on DPO designation and positioning. Its findings were qualitative rather than a single headline percentage, but recurring themes were insufficient DPO resourcing, insufficient training and expertise, and unresolved conflicts of interest — suggesting that appointment alone does not guarantee an effectively functioning role.

11 Employee GDPR Training

84%

of cyberattacks involve a social-engineering component (context indicator, not a training-coverage rate)

ENISA, Cybersecurity for SMEs: Challenges and Recommendations, 2021

This is the weakest-evidenced dimension in the report. No EU-specific, GDPR-focused, business-wide training-coverage statistic — comparable to “X% of employees received GDPR training in the past 12 months” — could be verified from Cisco, KnowBe4, Proofpoint, or ENISA sources in this research pass. ENISA's SME cybersecurity guidance notes qualitatively that awareness and training are often deprioritized under staff and budget constraints, and that the large majority of attacks involve a social-engineering element, which underscores why training matters without measuring how much of it actually happens.

A claim that DLA Piper found GDPR-trained organizations had 40% fewer reportable breaches surfaced during research but could not be traced to any DLA Piper publication; it is excluded here as unverified and should not be repeated elsewhere.

■ *DATA GAP — No current, EU-specific, business-wide GDPR training-coverage percentage was located. TrustArc's 2025 Global Benchmarks Report (n=1,775) and Proofpoint's State of the Phish report likely contain a usable figure; recommended as a direct follow-up for a future edition of this report.*

Cross-Cutting Themes & Conclusion

Three patterns recur across all eleven dimensions. First, **documentation consistently lags intent**: organizations broadly accept GDPR's requirements in principle — most appoint a DPO where required, most claim awareness of RoPA and DPIA obligations — but the paperwork and process discipline behind that intent (complete records, full vendor vetting, tested incident-response plans) is thinner and harder to measure. Second, **SME resourcing is the sharpest fault line** in nearly every dataset that breaks out firm size: SMEs lag on SCC adoption, DPO staffing intensity, and general vendor risk management, echoing ENISA's finding that awareness and training are the first casualties of a constrained budget. Third, **governance is structurally behind the newest risk surface**: AI adoption and third-party/SaaS sprawl are both outpacing the formal governance built to manage them, with double-digit-point gaps between usage and oversight in both areas.

The clearest finding of this synthesis, however, is a research gap rather than a compliance gap: current (2023–2026), EU-specific, business-wide statistics are genuinely scarce for several core obligations — RoPA completeness, DPIA coverage, incident-response readiness, and employee training chief among them. Where such data exists, it is often global or several years old. This is itself a finding worth acting on: the privacy industry's own measurement of GDPR compliance has not kept pace with the regulation's eighth year in force.

Recommendations for Businesses

- Treat RoPA and DPIA documentation as living processes, not one-time exercises — the 2018 baseline data suggests many organizations built partial records early on and never revisited them.
- Prioritize cookie consent remediation: it is the most heavily audited, most frequently enforced, and most fixable of the eleven dimensions, with a clear, well-documented compliance bar.
- Close the AI governance gap before it widens further — formalize an AI usage policy and GDPR/AI Act impact assessment process now, ahead of increasing regulatory scrutiny.
- Extend vendor due diligence to the full SaaS portfolio, not just top-tier vendors — with only roughly a third of vendors typically assessed, most third-party exposure goes unmeasured.
- Revisit international transfer mechanisms in light of the EU-US Data Privacy Framework and evolving EDPB guidance — the most recent EU-specific benchmark data predates these changes.
- Resource the DPO role adequately once appointed, not just formally — the EDPB's own enforcement review found under-resourcing and training gaps common even where a DPO is in place.

Full Source List

• IAPP / EY, *IAPP-EY Annual Governance Report* (Daily Dashboard survey, Oct–Nov 2018), n=410 GDPR-subject respondents. iapp.org

• IAPP / EY, *Privacy Governance Report 2024*, global privacy professionals. iapp.org/resources/article/privacy-governance-report

• IAPP, *AI Governance Profession Report 2025*, global privacy/AI governance professionals. iapp.org/resources/article/ai-governance-profession-report

• IAPP, *Study: An estimated 500K organizations have registered DPOs across Europe*. iapp.org/news/a/study-an-estimated-500k-organizations-have-registered-dpos-across-europe

• European Data Protection Board (EDPB), *Coordinated Enforcement Action — Designation and Position of Data Protection Officers*, January 2024, n=17,490 across 22 EEA authorities. edpb.europa.eu

• European Data Protection Board (EDPB), *Coordinated Enforcement Action — Use of Cloud-Based Services by the Public Sector*, January 2023. edpb.europa.eu

• European Data Protection Supervisor (EDPS), *DPIA Survey 2024 Report to EU Institutions, Bodies, Offices and Agencies*, September 2025. edps.europa.eu

• Ponemon Institute (sponsored by RiskRecon/Mastercard), *The 2022 Data Risk in the Third-Party Ecosystem Study*, n=1,162, North America and Western Europe. riskrecon.com

• Ponemon-Sullivan Privacy Report, *State of Third-Party Risk Assessments*, March 2026, n=1,465 (EMEA=431, US=632, APAC=402). ponemonsullivanreport.com

• Cisco, *2025 Data Privacy Benchmark Study*, n=2,600 across 12 countries. cisco.com

• DLA Piper, *GDPR Fines and Data Breach Survey*, 8th annual edition, January 2026, 31-country supervisory-authority data. dlapiper.com

• ENISA, *Cybersecurity for SMEs: Challenges and Recommendations*, 2021. enisa.europa.eu

• TrustArc, *2025 Global Privacy Benchmarks Report*, n=1,775. trustarc.com

• Nouwens, Kristensen, Maalt & Bagge, “A Cross-Country Analysis of GDPR Cookie Banners,” *ACM CHI 2025 Conference Proceedings*, n=254,148 websites across 31 EU/EEA countries. dl.acm.org

• UK Information Commissioner's Office (ICO), cookie compliance review, January 2025 (top-1,000 UK website sweep, phase 2). ico.org.uk

• Privado.ai, *The State of Website Privacy Report*, November 2024, top 100 US/European sites. privado.ai

• Commission Nationale de l'Informatique et des Libertés (CNIL), enforcement actions and sanctions data, 2025. cnil.fr

• EY Law, *Data Subject Access Requests (DSARs): 2023 EY Law Survey*, n=500+, global financial services. ey.com

• Talend (via CIO Dive), DSAR deadline-compliance survey, December 2019. ciodive.com

• DataGrail, DSAR volume trend research, 2025/2026 editions. datagrail.io

• Hiscox, *Cyber Readiness Report 2025*, multi-country SME/mid-market survey. hiscoxgroup.com

• SecurityScorecard, *2025 Global Third-Party Breach Report*, global breach dataset. securityscorecard.com

• DIGITALEUROPE, *Schrems II Impact Survey Report*, 2020, n≈300 EU businesses. digitaleurope.org