Is Your Organization GDPR Ready Or Risking Everything?

A Strategic Compliance Resource for Decision-Makers Who Want Clarity, Not Confusion. If your organization touches EU/EEA citizen data 4 from anywhere in the world - GDPR applies to you.

CREST Registered Region - Global

VA PEN TEST

certin Empanelled

GDPR

General Data Protection Regulation

GDPR in Today's Business Landscape

The General Data Protection Regulation (GDPR) is one of the world's most comprehensive data privacy laws. It sets the global benchmark for how organizations must collect, process, protect, and manage personal data.

Global Applicability: GDPR applies to any organization that processes personal data of **EU/EEA residents**—regardless of where your organization is located. Physical presence in Europe is not required.

Why Executives Should Care

Protect Your Business
Avoid massive fines, legal actions, and regulatory investigations.

Build Customer Trust
Demonstrate that you value and protect personal data.

Accelerate Revenue Growth
GDPR compliance removes a major barrier in EU enterprise deals.

Operate Globally with Confidence
Ensure smooth cross-border data transfers and global operations.

Strengthen Governance
Implement better data practices, accountability, and risk management.

€20M / 4%
Maximum Penalty
Up to 620 million or 4% of global annual turnover—whichever is higher.

72 Hours
Breach Notification
Mandatory notification to the regulator within 72 hours of becoming aware of a breach.

8
Data Subject Rights
Individuals have enforeeable rights over their personal data at any time.

Cross-Border
Data Obligations
Strict rules govern transfers of personal data outside the EU/EEA.

Key GDPR Requirements Every Organization Must Know

Lawful & Fair Processing
Process data only on a valid legal basis.

Transparency & Notice
Provide clear, concise information about data processing.

Data Minimization
Collect only the data you truly need for specified proposes.

Security & Confidentiality
Implement appropriate technical and organizational measures.

Storage Limitation
Retain data only for as long as necessary for the purpose.

Accountability & Documentation
Maintain records and demonstrate compliance.

The Bottom Line: GDPR is not just a regulatory requirement—it is a business imperative. Compliance protects your organization from financial, operational, and reputational risks while opening doors to EU markets and partners.

Understanding GDPR Fundamentals

GDPR sets clear rules for how personal data must be handled. Knowing the key roles, lawful bases, and core principles is the foundation of a strong compliance program.

Data Controller
Your Organization

Determines the purpose and means of processing personal data.
You decide why data is collected and how it is used.
Ultimate accountability lies here.

- Defines processing purposes
- Holds primary regulatory accountability
- Signs Data Processing Agreements with vendors
- Responds to Data Subject Access Requests

Instructions
Purpose, Data, Processing Rules

Processing
On Behalf of Controller

Data Processor
Your Vendors & Partners

Processes personal data only on your documented instructions and under a signed DPA.

- Processes data per Controller's instructions
- Must notify Controller of breaches immediately
- Cannot subcontract without Controller approval
- Equally liable under QDPR for their processing

6 Lawful Bases for Processing Personal Data

1	**Consent**	Freely given, specific, informed, and unambiguous. Must be as easy to withdraw as to give. Pre-ticked boxes are not valld consent.
2	**Contract**	Processing necessary to fulfill a contract with the individual, or to take pre-contractual steps at their request.
3	**Legal Obligation**	Processing required to comply with EU or member state law (e.g., tax records, employment law obligations).
4	**Vital Interests**	Processing necessary to protect someone's life. Rarely applicable outside healthcare and emergency scenarios.
5	**Public Task**	Processing in the exercise of official authority or public interest functions. Primarily for public sector organizations.
6	**Legitimate Interests**	Processing necessary for your legitimate interests — unless overridden by the individual's rights and freedoms. Requires a documented Legitimate interests Assessment (LIA).

GDPR Core Principles You Must Follow

Lawfulness, Fairness & Transparency
Process data legally, fairly, and transparently.

Purpose Limitation
Collect data for specific, clear, and legitimate purposes.

Data Minimization
Collect only the data you truly need.

Accuracy
Keep personal data accurate and up to date.

Storage Limitation
Retain data only for as long as necessary for the purpose.

Integrity & Confidentiality
Protect data using appropriate security measures.

Accountability
Demonstrate compliance with policies, processes, and documentation.

Key Takeaway: Understanding these foundations helps you make the right compliance decisions, build stronger controls, and demonstrate accountability to regulators, customers, and partners.

Data Subject Rights & Your Responsibilities

GDPR gives individuals powerful rights over their personal data. Your organization must have the right processes, tools, and timelines to honor these rights—every time.

Legal Obligation

These rights are enforceable by law. Failure to comply can result in regulatory action and significant financial penalties.

The 8 Rights Under GDPR

1. Right to Be Informed

Individuals have the right to claar, transparent, and easily accessible information about how their personal data is collected, used, and protected.

2. Right of Access (DSAR)

Individuals can request access to all personal data you hold about them. You must respond within 30 days.

3. Right to Rectification

Individuals can request correction of inaccurate or incomplete personal data without undue delay.

4. Right to Erasure

Also known as the "Right to be Forgotten". You must delete personal data when there is no legitimate reason to retain it.

5. Right to Restrict Processing

Individuals can request the restriction of processing while a dispute or verification is underway.

6. Right to Data Portability

Individuals can receive their personal data in a structured, commonly used, machine-readable format and transmit it to another organization.

7. Right to Object

Individuals can object to processing based on legitimate interests or for direct marketing—and you must stop.

8. Rights Related to Automated Decision-Making

Individuals can challenge decisions made safely by automated means, including profiling, and request human review.

DSAR (Data Subject Access Request) Workflow

1. **Request Received** — Through email, portal, or other channels.
2. **Verify Identity** — Confirm the identity of the requestor.
3. **Locate & Retrieve Data** — Search all relevant systems and third-party processors.
4. **Review & Redact** — Remove data of others and apply legal exemptions if applicable.
5. **Respond to Individual** — Provide data in a structured, commonly used format within 30 days.
6. **Document & Track** — Maintain records of the request and response for ausi't purposes.

Response Timeline: Respond within 30 days of receiving the request.
In complex cases, you may extend by up to 60 additional days with valid justification and prior notice to the individual.

30 Days
Standard Response Time

Respond to DSARs within 30 days. Extensions up to 90 days for complex or high-volume requests.

50+
Average DSARs / Month

Typical volume for mid to large enterprises. Without proper processes, this becomes a compliance risk.

€200 – €500
Avg Cost Per Manual DSAR

Manual handling is time-consuming and expensive across multiple teams and systems.

High Risk
Regulatory Exposure

Unanswered or delayed DSARs are one of the top reasons for GDPR fines.

Decision-Maker Takeaway: Every DSAR is a legal obligation, not an IT ticket. Strong processes, automation, and cross-functional coordination are essential to protect your organization from regulatory action and reputational damage.

The Real Cost of Non-Compliance

GDPR enforcement is intensifying. Fines are higher, investigations are longer, and no organization is too big—or too small—to be targeted.

The Question is Not
"Can we afford to comply?"
It's
"Can we afford not to?"

Landmark GDPR Fines – The Enforcement Record

Meta	amazon	WhatsApp	Google	H&M
€1.2 Billion	**€746 Million**	**€225 Million**	**€90 Million**	**€35 Million**
2023	**2021**	**2021**	**2022**	**2020**
Unlawful cross-border data transfers to the US. Largest GDPR fine in history.	Advertising targeting system violations.	Transparency failures: users were not adequately informed about data sharing with Meta group companies.	Cookie consent failures on YouTube. Consent mechanism was not freely given.	Unlawful employee monitoring and excessive data retention.
Irish DPC	Luxembourg DPA	Irish DPC	French CNIL	Hamburg DPA

Your Full Risk Exposure – Beyond the Fine

Regulatory Fines
Up to €20M or 4% of annual global turnover – whichever is higher. Calculated on worldwide revenue, not just EU revenue.

Compensation Claims
Data subjects can seek compensation for material and non-material damages. Class actions are rising across EU countries.

Regulatory Investigations
DPA Investigations can last 18–38 months, consuming significant executive, legal, and operational resources—even if no fine is issued.

Reputational Damage
Fines are public record. Media coverage, customer churn, and brand eroxion can for exceed the financial penalty.

Loss of EU Market Access
Supervisory authorities can ban or restrict processing of EU citizen data—effectively blocking your access to the EU market.

The Math Is Unambiguous: Compliance Is Risk Insurance With Revenue Upside

Cost of a Compliance Program

€50K – €500K
One-time investment
+ €20K – €100K
Ongoing Annual Investment
Includes assessment, policy framework, technical controls, training, and continuous monitoring.

VS

Cost of a Single Major Fine

€1M – €20M+
Fine Alone
+ Additional Hidden Costs
Investigation costs + Legal defense + PR crisis management + Customer churn + Contract terminations

CFO Perspective
GDPR compliance is not a cost center — it is risk. adjusted capital allocation. Model it as insurance with a known premium against an open-ended liability.

CEO Perspective
78% of EU enterprise procurement teams now require documented GDPR compliance evidence before signing contracts. Non-compliance costs you deals before regulators ever get involved.

Key Takeaway: The cost of non-compliance is unlimited. The cost of compliance is predictable. The choice is simple. The impact is lasting.

Your GDPR Compliance Roadmap

A proven, six-phase approach to bulid a defensible, sustainable, and audit-ready GDPR compliance program.

Our Promise

A pragmatic, business-aligned journey that reduces risk, strengthens trust, and accelerates growth.

The 6-Phase GDPR Compliance Journey

1 — Discover
Map Your Data
Identify all personal data, sources, systems, data flows, vendors, and cross-border transfers.
Weeks 1–3

2 — Assess
Identify Gaps
Evaluate current practices against ODPR requirements and assess risks and priorities.
Weeks 2–5

3 — Govern
Build Framework
Establish policies, lawful basis, privacy notices, DPAs, governance structure, and DPO support.
Weeks 3–7

4 — Secure
Implement Controls
Deploy technical controls, encryption, access management, DLP, and breach detection.
Weeks 4–9

5 — Implement
Operationalize
Roll out procedures, DSAR workflow, training, DPIAs, and vendor risk management.
Weeks 6–12

6 — Monitor
Assure & Improve
Continuously monitor, test, and improve with dashboards, audits, and regulatory readiness.
Weeks 10–16

Typical Timeline by Organization Size

Startups & SMBs
12 – 16 Weeks
- Focused scope and lean team
- Rapid deployment of core controls
- Documentation & foundational compliance

Mid-Market
16 – 24 Weeks
- Multiple business units & processes
- Vendor and data landscape mapping
- Cross-functional alignment & training

Enterprise
20 – 32 Weeks
- Complex data environments
- International operations
- Legacy systems & governance integration

Key Outcomes You Will Achieve

Risk Reduction
Minimize regulatory, financial, and reputational risk.

Regulatory Readiness
Be prepared for audits, investigations, and regulatory requests.

Customer Trust
Demonstrate privacy leadership and strengthen relationships.

Business Growth
Remove compliance barriers and win more EU enterprise deals.

Operational Efficiency
Standardize processes and automate where it matters.

Continuous Compliance
Sustain compliance with monitoring, metrics, and improvements.

Key Takeaway: GDPR compliance is not a one-time project—it is a continuous program. Our roadmap ensures you build the right foundation, implement the right controls, and maintain confidence in your compliance posture—every day.

Result: A defensible posture that satisfies regulators, reassures customers, and drives business forward.

A Complete GDPR Compliance Solution

We deliver end-to-end GDPR compliance—combining people, process, and technology—to help you build a privacy-first organization that is secure, accountable, and audit-ready.

Our Promise

Practical. Measurable. Sustainable.

Everything we deliver is designed for real-world implementation and regulatory defensibility.

Key Deliverables

Technical Controls

- Data discovery & classification
- Consent management framework
- Encryption (at rest & in transit)
- Access control & RBAC
- Data Loss Prevention (DLP)
- Pseudonymization & enenymization
- Breach detection & 72-hour notification workflow
- DSAR automation & Tracking
- Cross-border transfer mechanisms
- Vendor & processor risk assessment

Policies & Governance

- GDPR-compliant Privacy Policy
- Record of Processing Activities (ROPA)
- Data Protection Impact Assessment (DPIA)
- Data Processing Agreement (DPA) templates
- Data Subject Rights procedures
- Data Retention & Deletion Policy
- Incident Response & Breach Notification Plan
- Employee training & awareness
- Vendor assessment & management framework

Framework Reuse – Maximize Your Investment

60% — **GDPR + ISO 27001**
Up to 60% of controls overlap, Fast-track your ISO 27001 certification.

50% — **GDPR + SOC 2**
Up to 50% overlap. Strengthen your SOC 2 Type 5 readiness.

55% — **GDPR + DPDPA (India)**
Up to 55% overlap with India's Digital Personal Data Protection Act.

45% — **GDPR + HIPAA**
Up to 48% overlap for healthcare organizations.

Why 540+ Organizations Trust Briskinfosec

540+ — **Clients Served**
Across enterprise, mid-market, and high-growth companies in 17 countries.

4,800+ — **Security Projects**
Delivered across cybersecurity, privacy, and compliance disciplines.

98%+ — **Client Renewal Rate**
Reflecting the quality and sustained value of our engagements.

40% — **Faster Compliance**
Average reduction in time-to-compliance vs. clients' prior internal attempts.

17 — **Countries Served**
Across Americas, Europe, Middle East, Asia-Pacific, and beyond.

60% — **Audit Cost Reduction**
Average reduction in audit preparation costs after Year 1.

Why Briskinfosec is the Right Partner

Dual Expertise: Security + Privacy Law
We combine deep cybersecurity skills with privacy law expertise for true end-to-end GDPR compliance.

CREST Accredited
Our assessments and testing are independently verified to international standards.

Certified & Experienced Team
Experts with OSCP, CISSP, CISA, CRISC, CEH, CDPO, and ISO 27001 Lead Auditor/Implementer credentials.

Industries We Serve

- SaaS & Cloud
- ForTech & Banking
- HealthTech & Pharma
- E-Commerce & Retail
- EdTech
- Manufacturing
- IT Services & BPOs

Client Outcomes – Real Results

> A 200-person SaaS company achieved full GDPR nompliance in just 14 weeks and closed their first EU Fortune SDD deal within 3 months of receiving their compliance documentation package from Briskinfosec. It.
>
> **— SaaS Client,**
> Global -- EU Market Expansion

> A global IT services firm reduced DSAR response time from 15 days to 48 hours using our DSAR automation implementation --and retained a critical £2M EU managed services contract that had been at risk.
>
> **— IT Services Client,**
> EU Contract Retention

The Bottom Line: We don't just help you check the compliance box—we build a resillent, privacy-first foundation that protects your organization and accelerates your business in the EU and beyond.

What Happens Next?

Client Breaches
Post-assessment security record

Start With Zero Commitment

Understanding your unique security challenges begins with a conversation. We offer a no-obligation consultation to assess your current posture and identify immediate risk areas.

Our Team Holds Industry-Leading Certifications

We invest heavily in our team's continuous education because the threat landscape never stops evolving. Neither do we.

OSCP | OSWE | CISSP | CISA | CEH

CREST Accredited
Internationally certified penetration testing excellence

CERT-IN Empanelled
Government-recognized trusted cybersecurity assessment provider

ISO 27001 : 2022 Certified
Our own security practices are independently audited and verified annually

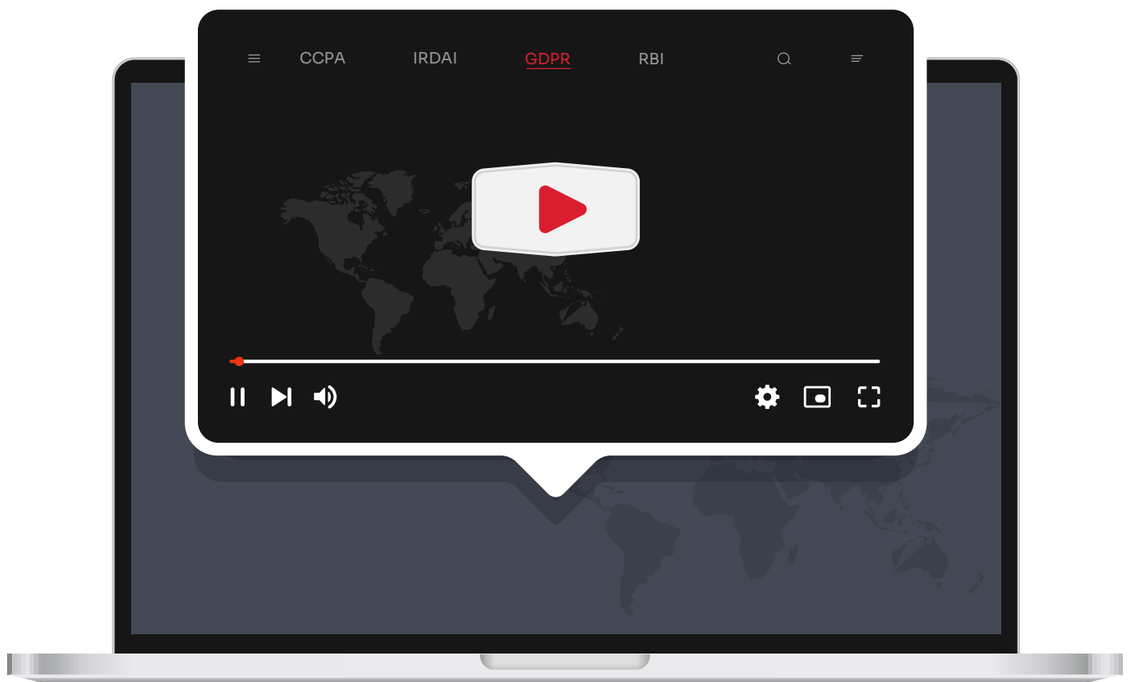
25+
Countries Client Portfolio

67%
Logic flaws missed by bots

98%
Client retention

640+
Successful Customers

5600+
Delivered in 24 countries



Reach us for FREE
consultation

Book Now

sales@briskinfosec.com
www.briskinfosec.com

Our Geographical Presence India UAE