

GDPR & GLOBAL PRIVACY REGULATION.

GDPR applies to any organization processing an EU resident's personal data, regardless of where that organization is actually based. **Consent is only one of six lawful bases, and defaulting to it for everything often creates more compliance risk, not less.**

- EXTRATERRITORIAL REACH
- LAWFUL BASIS
- 72-HOUR BREACH NOTIFICATION
- CROSS-BORDER TRANSFERS

01 THE MECHANISM



Extraterritorial Reach, Not Just an EU Law

GDPR applies to any organization processing an EU resident's personal data **regardless of where that organization is based**, so a company with no EU office can still be fully subject to it.



Six Lawful Bases, Not Just Consent

Every processing activity needs a valid legal basis, and consent is often not the most appropriate one; **contract and legitimate interests frequently apply instead.**



72 Hours to Notify a Breach

Organizations must notify their supervisory authority within 72 hours of becoming aware of a breach, **a timeline many internal IR processes weren't originally built around.**

02 THE FLOW

The Compliant Data Program CONTAINED

1

Each processing activity is mapped to a **specific, documented lawful basis before it begins**, and privacy is built into new systems from the design stage.

2

A data subject's access or erasure request is routed through a defined process that **fulfills it within the required timeframe**, across every system that holds their data.

3

A detected breach triggers the **72-hour notification clock immediately**, with a documented process ready to assess risk and notify on time.

The Reactive, Undocumented Program EXPOSED

1

Processing activities were never mapped to a specific lawful basis, so when a regulator asks, there's **no documented justification** for how the data is being used.

2

A data subject's erasure request gets fulfilled in the system someone remembers, while data **quietly persists in a backup or a spreadsheet** nobody tracked.

3

A breach is discovered internally but sits in an ad hoc escalation process for days before anyone realizes the **72-hour window has already passed.**

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Lawful Basis Documentation	Mapping every processing activity to one of six valid legal bases, chosen deliberately rather than defaulting to consent for everything.
Data Subject Rights Fulfillment	A defined process to actually locate, correct, export, or erase an individual's data across every system within the required timeframe.
Breach Notification Readiness	A documented process to assess, notify the supervisory authority within 72 hours, and inform affected individuals when required.
Cross-Border Transfer Mechanisms	Standard Contractual Clauses, adequacy decisions, or Binding Corporate Rules governing personal data moved outside the EEA.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Defaulting to Consent for Every Processing Activity	No	Consent is only one of six lawful bases, and it's not always the most appropriate or legally durable choice for a given activity.
Assuming GDPR Only Applies to EU-Based Companies	No	GDPR's extraterritorial reach covers any organization processing an EU resident's data, regardless of where it's located.
Treating GDPR Compliance as Global Privacy Compliance	No	Other jurisdictions, like California's CCPA/CPRA and Brazil's LGPD, have their own distinct requirements GDPR doesn't automatically satisfy.
International Data Transfers With No Documented Safeguard	No	Moving personal data outside the EEA without an adequacy decision, SCCs, or BCRs is a direct compliance gap, not just a best-practice miss.
Lawful Basis Mapping + Rights Fulfillment + Breach Readiness + Transfer Mechanisms	Yes	Covers the legal justification, the individual's enforceable rights, the incident timeline, and the cross-border reality together.

GDPR & GLOBAL PRIVACY REGULATION. JUSTIFY · FULFILL · NOTIFY

05 PROGRAM OPERATIONS

GDPR's extraterritorial reach is one of its most consequential and least understood features — a company never based in the EU can still be fully subject to it based purely on whose data it processes.

Consent is not the default answer. Many processing activities are more appropriately and durably justified under contract or legitimate interests, and defaulting to consent everywhere often creates more risk.

The 72-hour breach notification clock starts at awareness, not confirmation, which is why a documented, rehearsed escalation process matters as much as detection capability itself.

Fines scale off global annual turnover, not just EU revenue, and the maximum tier applies whichever calculation — percentage or flat amount — is higher.

06 CONTROL MAPPING

GDPR (EU 2016/679)

The foundational regulation itself, defining lawful bases, data subject rights, breach notification timelines, and enforcement structure.

STANDARD CONTRACTUAL CLAUSES (SCCS)

The European Commission's approved contractual mechanism for lawfully transferring personal data outside the EEA.

SCHREMS II RULING

The Court of Justice of the EU decision invalidating the EU-US Privacy Shield, requiring supplementary safeguards for many EU-US data transfers.

GLOBAL PRIVACY LAW PATCHWORK

Related but distinct regimes, including California's CCPA/CPRA, Brazil's LGPD, and China's PIPL, each with their own separate requirements.

07 WHAT THIS DOES NOT SOLVE

Compliance in Other Jurisdictions

Meeting GDPR's requirements **doesn't automatically satisfy** CCPA, LGPD, PIPL, or any other jurisdiction's distinct privacy law.

Data Security Itself

GDPR requires appropriate security measures, but **being lawfully compliant on paper doesn't substitute** for an actual, effective security program.

Third-Party Processor Practices

A signed Data Processing Agreement establishes legal obligations, but **doesn't guarantee a processor's actual technical controls** meet the standard it describes.

Evolving Legal Interpretation

Cross-border transfer mechanisms and enforcement priorities have **shifted meaningfully since 2018** and continue to evolve.

08 MYTHS VS. REALITY

MYTH "GDPR only applies to companies based in the EU."	REALITY GDPR applies to any organization processing an EU resident's personal data, regardless of where that organization is actually located.
MYTH "Getting consent covers any data processing activity."	REALITY Consent is one of six lawful bases, and it's often not the most appropriate choice; contract and legitimate interests frequently apply instead.
MYTH "Being GDPR compliant means we're compliant everywhere."	REALITY Other jurisdictions like California and Brazil have their own distinct privacy laws that GDPR compliance doesn't automatically satisfy.
MYTH "The 72-hour clock starts once we've confirmed the full scope of a breach."	REALITY It starts at awareness of the breach, not full confirmation, which is why a fast, documented escalation process matters.
MYTH "GDPR fines are capped at a small, predictable amount."	REALITY The maximum tier is up to 4% of global annual turnover or €20 million, whichever is higher, calculated off global revenue.

09 SPEAK THE PROGRAM — KEY TERMS

DATA CONTROLLER

The entity that **determines the purposes and means** of processing personal data.

DATA PROCESSOR

An entity that processes personal data on behalf of a controller, **carrying its own direct legal obligations** under GDPR.

LAWFUL BASIS

One of six legally valid justifications required for any processing of personal data, **of which consent is only one.**

DATA SUBJECT RIGHTS

Enforceable rights individuals hold over their own data, including **access, rectification, erasure, and portability.**

STANDARD CONTRACTUAL CLAUSES (SCCS)

The European Commission's approved contract terms for **lawfully transferring personal data outside** the EEA.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

A mandatory formal risk assessment for processing **likely to result in high risk to individuals.**