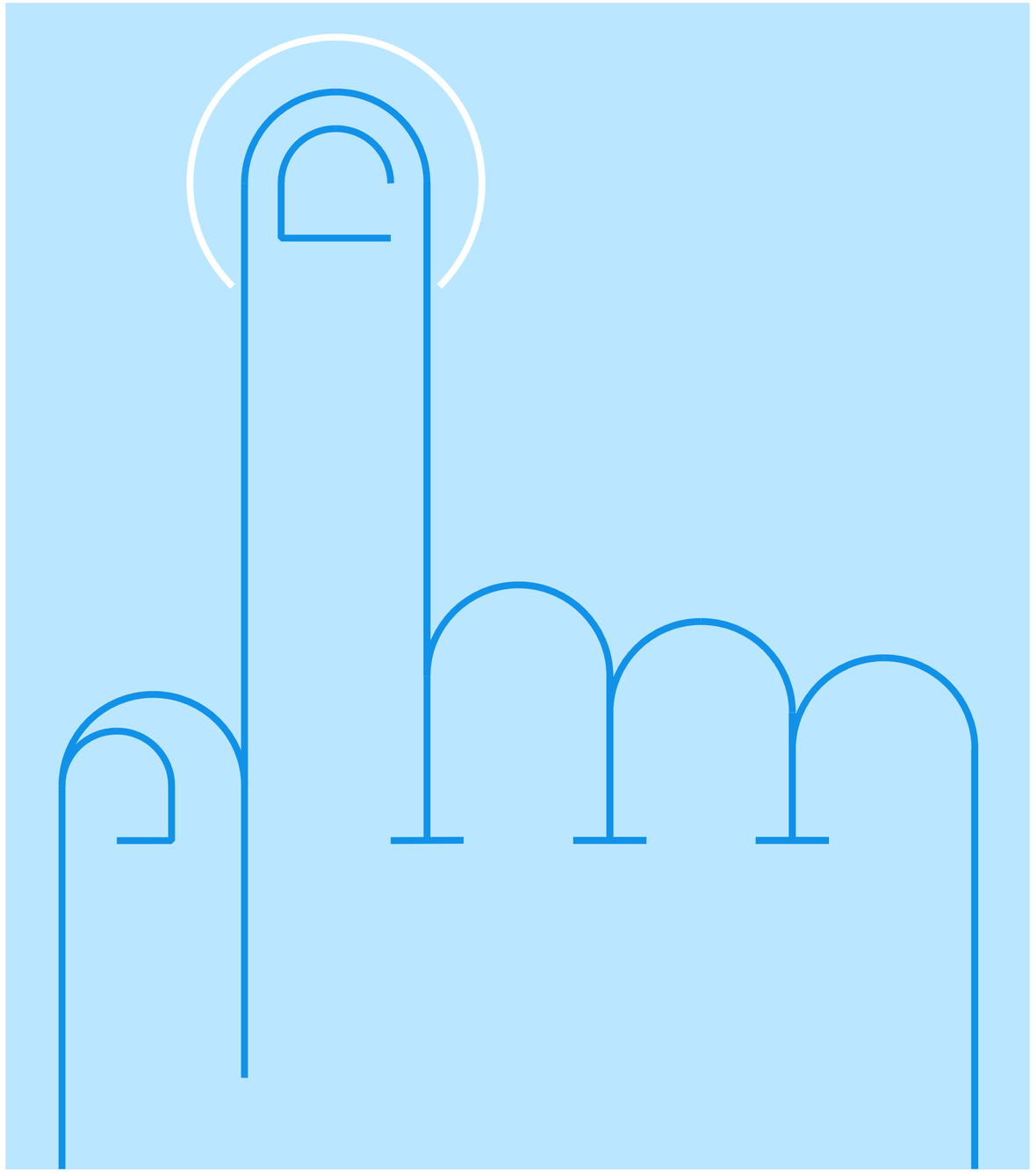
From checkboxes to compliance & trust

Consent Management in Personal Data Protection



Do you really read the terms before clicking?

Consent is not just legal compliance — it’s the foundation of trust.

Why Consent Matters

Business risks.

- Violations can mean fines up to 2% of annual revenue (Pasal 57), or up to Rp50–60m for corporates (Pasal 67–70)
- Loss of trust → customers churn.
- Reputation damage → media, social backlash.

Law requires it.

- Indonesia PDP Law (UU 27/2022): Consent must be explicit, documented, withdrawable.
- GDPR & PDPA: Consent must be freely given, informed, specific, and unambiguous.

Reality

- Most users just click blindly.
- Regulators say: companies must *still* prove valid consent.

Local Case (Indonesia)

“I never agreed to this” — when users complain

Imagine a bank or fintech runs an SMS or WhatsApp marketing campaign without getting a clear opt-in from customers. Some recipients feel annoyed and file complaints to OJK or Kominfo. The regulator then asks the company: *“Show us when and how these customers gave their consent.”* The company scrambles, but all it has is a generic “Agree to terms” record from account signup — no timestamp, no version of the consent text, and no separate opt-in for marketing. This puts the company at risk of violating the PDP Law, facing administrative fines of up to 2% of annual revenue, blocked marketing campaigns, and serious reputational damage.

More information:
UU 27/2022 →
BRTI →

Ministry of Communication and Information

Manages **Aduan BRTI**, a public portal where people can report spam SMS/WhatsApp.

If enough complaints are made against a number, KOMINFO can:

- Block the sender’s number.
- Order the telco or platform to stop the activity.
- Investigate whether PDP Law obligations were violated.

A generic ‘Agree to terms’ isn’t enough. Without timestamps, consent versions, and clear opt-ins, companies risk PDP Law violations and fines.

Who Asks, and When

Regulators don’t ask every day, but when they do, the stakes are high.

Who?

- **Kominfo** → PDP Law enforcement, spam/data complaints.
- **OJK** → banks, insurers, fintech (telemarketing).

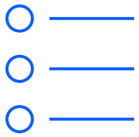
When?

- Customer complaints: *“I never consented.”*
- Data breaches: *“Why did you have this data?”*
- Audits: checks in high-risk sectors.
- Enforcement: after prior violations.

“Prove it.” That’s the standard.

Valid Consent Record

- Timestamp of when it was given
- Version of consent text shown
- Clear opt-in (not bundled with T&Cs)



Withdrawal Option

- User can revoke consent anytime
- Company must honor it quickly

Audit Trail

- Who consented, for what purpose, and how

Source: UU 27/2022, Articles 20–22, 55–56 (Indonesia Personal Data Protection Law).

Consent isn’t just compliance — it’s trust.

1

Trust & Reputation

Transparency shows respect for users → stronger brand value.

2

Smarter Personalization

Clear opt-ins let companies tailor offers confidently and responsibly.

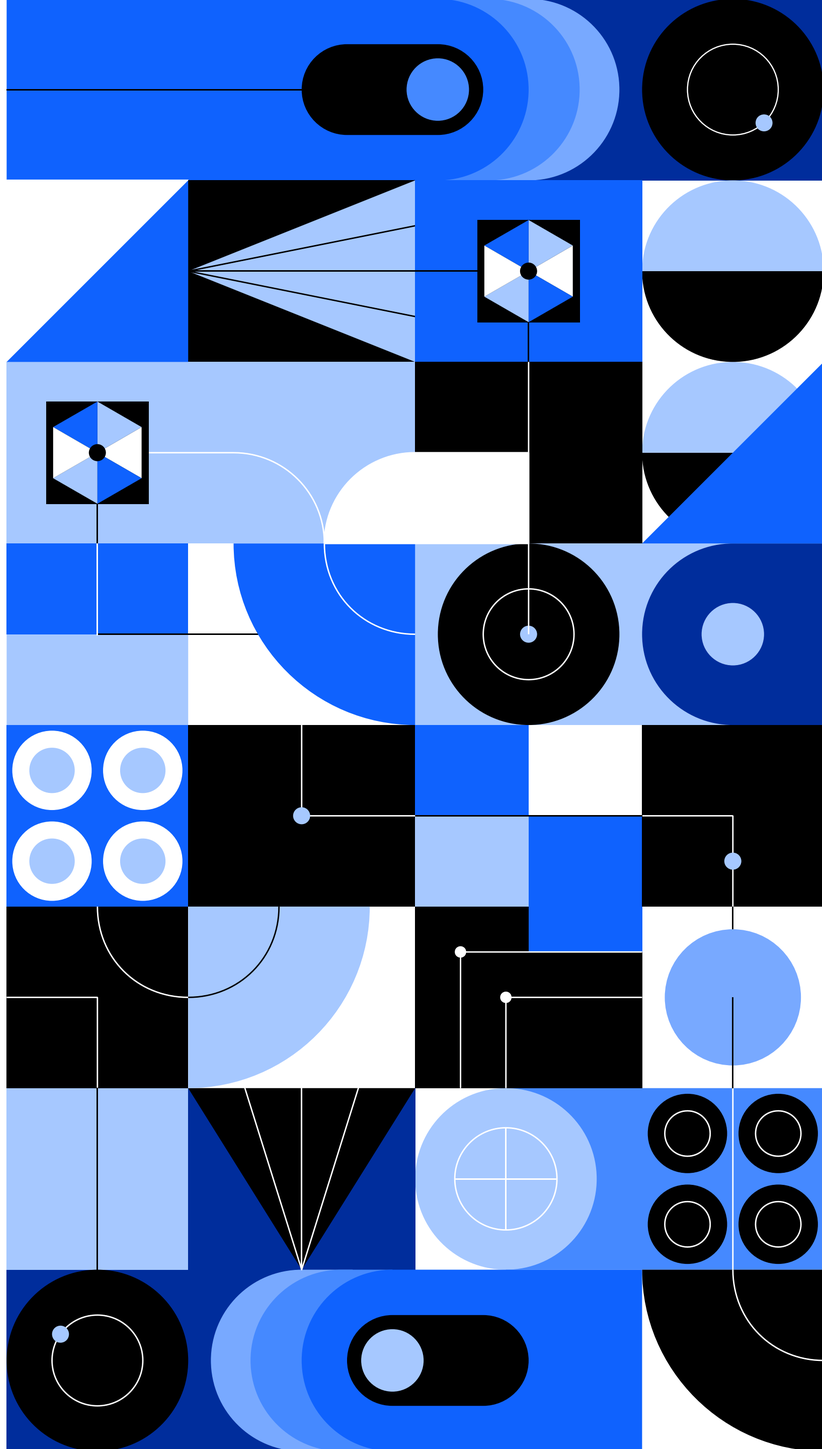
3

Efficiency & Loyalty

Fewer complaints and faster audits → lower risk, less churn, more satisfied customers.

Demo: IBM Verify Consent Management:

From legal risk to trusted user experience.



From checkboxes to compliance & trust