# GDPR Compliance Checklist

Checklist · 96 items · 15 sections

A working GDPR compliance checklist for controllers and processors operating in or targeting the EU. Built around Regulation (EU) 2016/679, EDPB guidelines, and ICO/CNIL guidance. Covers Article 30 ROPA, Article 13/14 notices, Article 35 DPIAs, Chapter V transfers (post-Schrems II), breach notification, and Article 28 vendor agreements with real fine tiers and enforcement precedents.

Open the editable version online:
https://genechecklist.com/checklist/gdpr-compliance-checklist

## APPLICABILITY AND TERRITORIAL SCOPE (ARTICLE 3)

- [ ] Confirm whether you offer goods or services to EU/EEA data subjects (Article 3(2)(a))
  HIGH
  *Paid plans in EUR or EU-language marketing triggers extraterritorial scope.*
- [ ] Determine whether you monitor EU residents via cookies, analytics, or behavioural tracking (Article 3(2)(b))
  HIGH
- [ ] Classify your role per processing activity: controller, processor, or joint controller
  HIGH
- [ ] Confirm whether UK presence triggers parallel UK GDPR + Data Protection Act 2018 obligations
  HIGH
- [ ] Designate an EU representative under Article 27 if you have no EU establishment but target EU users
  HIGH
  *Document name, EU address, and mandate in writing.*
- [ ] Identify the lead supervisory authority for one-stop-shop where the main establishment sits (Article 56)

## LAWFUL BASIS FOR PROCESSING (ARTICLE 6)

- [ ] Document a lawful basis per distinct processing purpose (Article 6: consent, contract, legal obligation, vital interests, public interest, legitimate interests)
  HIGH
- [ ] Use contract (6(1)(b)) for account creation, paid service delivery, payment processing
  HIGH
- [ ] Use legal obligation (6(1)(c)) for tax records and lawful authority requests

HIGH

- [ ] Use legitimate interests (6(1)(f)) for fraud prevention, security logs, basic analytics

  HIGH

  *Run and document a 3-part LIA (Legitimate Interest Assessment): purpose, necessity, balancing.*

- [ ] Use consent (6(1)(a)) for marketing email, non-essential cookies, optional sharing

  HIGH

  *Must meet Article 7 conditions.*

- [ ] For genetic, health, or other special-category data, identify a separate Article 9(2) condition

  HIGH

  *Explicit consent under 9(2)(a) is the default; alternative research/public-interest grounds may apply.*

- [ ] Never rely on consent where a power imbalance exists (EDPB Guidelines 05/2020)

  HIGH

- [ ] Maintain a lawful-basis register linking each purpose to its Article 6 and (where applicable) Article 9 ground

## RECORDS OF PROCESSING ACTIVITIES (ARTICLE 30)

- [ ] Maintain a written ROPA even below 250 employees if you process special-category data

  HIGH

  *Article 30(5) exemption carve-out applies.*

- [ ] ROPA controller record: name, contact, purposes, subject categories, data categories, recipients, transfers, retention, TOMs (Article 30(1))

  HIGH

- [ ] ROPA processor record: controller name, categories of processing, sub-processors, transfers, security measures (Article 30(2))

  HIGH

- [ ] Make the ROPA available on request to the supervisory authority (Article 30(4))

  HIGH

- [ ] Review the ROPA at least every 12 months and on any new feature launch, vendor change, or category expansion

## PRIVACY NOTICE CONTENT (ARTICLES 13 AND 14)

- [ ] Publish a layered privacy notice at signup; link in footer; use plain language (Article 12(1))

  HIGH

- [ ] Include controller identity, EU representative, and DPO contact where applicable (13(1)(a)-(b))

  HIGH

- [ ] List each processing purpose with its lawful basis; state the interest pursued for legitimate interests (13(1)(c)-(d))

  HIGH

- [ ] List recipients and categories of recipients, including infrastructure, AI, payment, and analytics vendors (13(1)(e))

  HIGH

- [ ] Disclose third-country transfers and the safeguard relied on, with a link to the SCCs or adequacy decision (13(1)(f))

  HIGH

- [ ] State retention periods per data category, or the criteria used to determine them (13(2)(a))

  HIGH

- [ ] Inform data subjects of all Article 15-22 rights (13(2)(b))

  HIGH

- [ ] State the right to withdraw consent without affecting prior lawfulness (13(2)(c))

  HIGH

- [ ] State the right to lodge a complaint with a supervisory authority (13(2)(d))

  HIGH

- [ ] Disclose whether provision of data is statutory/contractual and consequences of refusal (13(2)(e))
- [ ] Disclose any automated decision-making including profiling, with meaningful info on logic and significance (13(2)(f))

  HIGH

- [ ] When data is obtained indirectly, comply with Article 14 within one month of collection; identify the source

  HIGH

## CONSENT MECHANICS (ARTICLE 7)

- [ ] Make consent freely given, specific, informed, unambiguous, evidenced by a clear affirmative act

  HIGH

- [ ] Reject pre-ticked boxes, opt-out flows, bundled consent, or cookie walls (EDPB Guidelines 05/2020; CNIL 2020-091)

  HIGH

- [ ] Capture granular consent per purpose: marketing, analytics, AI training-data use, special-category data

  HIGH

- [ ] Log proof of consent: timestamp, IP, consent string, banner version, exact text shown (Article 7(1))

  HIGH

- [ ] Provide a withdrawal mechanism as easy as the original consent path (Article 7(3))

  HIGH

  *Persistent 'Manage cookies' footer link; one-click email unsubscribe.*

- [ ] Re-collect consent whenever purposes materially change
- [ ] Treat ePrivacy Directive 2002/58/EC cookie rules as parallel: prior consent required before any non-essential tracker fires

HIGH

## DATA SUBJECT RIGHTS (ARTICLES 15-22)

- [ ] Build a DSAR intake (e.g., privacy@yourdomain.com) plus an in-product self-service export; verify identity proportionately

HIGH

- [ ] Respond within one calendar month of receipt; extendable by two further months with notification (Article 12(3))

HIGH

- [ ] Provide responses free of charge unless manifestly unfounded or excessive (Article 12(5))

HIGH

- [ ] Honour Access (Article 15): supply a copy plus Article 15(1) metadata

HIGH

- [ ] Honour Rectification (Article 16); notify recipients of corrections per Article 19

HIGH

- [ ] Honour Erasure / right to be forgotten (Article 17); respect legal-hold and accounting exceptions in 17(3)

HIGH

- [ ] Honour Restriction (Article 18): flag records and limit processing to storage

HIGH

- [ ] Honour Portability (Article 20) for consent- or contract-based data in a structured, machine-readable format (JSON default)

HIGH

- [ ] Honour Objection (Article 21): absolute for direct marketing; balancing test otherwise

HIGH

- [ ] Honour rights related to automated decision-making (Article 22) for any decisions with legal or similarly significant effects

HIGH

*Offer human review.*

- [ ] Operate a rights-request log: requestor, date, type, outcome, SLA timestamps

## DATA PROTECTION OFFICER (ARTICLES 37-39)

- [ ] Reassess DPO obligation quarterly (Article 37(1)(b)-(c): large-scale monitoring or special-category processing)

HIGH

- [ ] Appoint a DPO before scale thresholds are crossed (WP29 Guidelines on DPOs, WP243)

  HIGH
- [ ] Publish DPO contact details in the privacy notice; notify the supervisory authority (Article 37(7))
- [ ] Guarantee DPO independence, direct reporting to highest management, no conflict of interest, sufficient resources (Articles 38, 39)

  HIGH
- [ ] Document DPO duties: advising, monitoring compliance, cooperating with the authority, acting as contact point

## DATA PROTECTION IMPACT ASSESSMENTS (ARTICLE 35)

- [ ] Run a DPIA before launching any high-risk processing (AI-driven decisions, automated profiling, large-scale special categories)

  HIGH
- [ ] Use the CNIL PIA tool or ICO sample DPIA template as the baseline methodology
- [ ] Cover the 4 Article 35(7) DPIA elements: systematic description, necessity/proportionality, risk assessment, mitigations

  HIGH
- [ ] Consult the supervisory authority under Article 36 where residual risk remains high after mitigation

  HIGH
- [ ] Re-run the DPIA when scope, vendors, model providers, or data categories change

## INTERNATIONAL TRANSFERS (CHAPTER V)

- [ ] Map every transfer of personal data outside the EEA (US, India, etc.)

  HIGH
- [ ] Prefer adequacy decisions (Article 45): UK, Switzerland, Japan, S Korea, NZ, Argentina, Israel, Andorra, Guernsey, IoM, Jersey, Uruguay, Faroes; EU-US DPF for certified importers

  HIGH
- [ ] For non-adequate destinations, execute the 2021 modular SCCs (Commission Decision 2021/914) with the correct module

  HIGH
- [ ] Conduct a Transfer Impact Assessment per Schrems II (CJEU C-311/18) and EDPB Recommendations 01/2020

  HIGH

  *Evaluate importer law and surveillance exposure; add supplementary measures (e.g., EU-held encryption keys).*
- [ ] Use Binding Corporate Rules under Article 47 only after authority approval for intra-group transfers

- [ ] Limit reliance on Article 49 derogations (explicit consent, contract necessity) to occasional, non-systematic transfers

## BREACH NOTIFICATION (ARTICLES 33-34)

- [ ] Define a personal data breach per Article 4(12) covering confidentiality, integrity, and availability incidents

  HIGH

- [ ] Notify the lead supervisory authority within 72 hours of becoming aware (Article 33)

  HIGH

  *Include categories and approximate numbers of subjects/records, likely consequences, and mitigations.*

- [ ] If notification is later than 72 hours, provide reasons for delay (Article 33(1))

  HIGH

- [ ] Notify affected data subjects without undue delay if the breach is likely to result in a high risk (Article 34)

  HIGH

  *Use plain language and concrete advice.*

- [ ] Maintain an internal breach register for every incident, even non-notifiable ones (Article 33(5))

  HIGH

- [ ] Run tabletop breach exercises at least annually covering key vendor incident vectors

## SECURITY OF PROCESSING (ARTICLE 32)

- [ ] Apply pseudonymisation and encryption in transit (TLS 1.2+) and at rest for all personal data stores

  HIGH

- [ ] Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems (32(1)(b))

  HIGH

- [ ] Provide ability to restore availability and access after an incident (32(1)(c)); test backups quarterly

  HIGH

- [ ] Adopt a process for regularly testing and evaluating effectiveness of TOMs (32(1)(d)); pen test annually

  HIGH

- [ ] Enforce least-privilege access and secrets management

  HIGH

- [ ] Train all personnel with access to personal data at onboarding and annually thereafter

## VENDOR AND PROCESSOR MANAGEMENT (ARTICLE 28)

- [ ] Sign an Article 28 Data Processing Agreement with every processor (infrastructure, AI, payments, analytics, email, error monitoring)

  HIGH

- [ ] Verify the DPA covers all 8 Article 28(3) elements: subject-matter, duration, nature, purpose, types of data, subject categories, controller obligations and rights

  HIGH

- [ ] Require written prior authorisation or general authorisation with change notice for sub-processors (Article 28(2))

  HIGH

- [ ] Flow down equivalent obligations to sub-processors (Article 28(4))

  HIGH

- [ ] Reserve audit and inspection rights; accept third-party audit reports (SOC 2 Type II, ISO 27001)
- [ ] Confirm each processor's transfer mechanism (DPF, SCCs, BCRs); obtain copies of executed SCCs
- [ ] Re-evaluate vendor compliance annually and on any material change

## CHILDREN'S DATA (ARTICLE 8)

- [ ] Block under-16 signups by default in information-society services (Article 8)

  HIGH

  *Lower only where the member state legislated a lower digital age: IE 16, FR 15, DE 16, ES 14, UK 13.*

- [ ] Where minors are permitted, obtain verifiable parental consent; document the verification method

  HIGH

- [ ] Write notices to under-18s in age-appropriate language (ICO Age Appropriate Design Code); avoid default profiling of minors

## DATA MINIMISATION, ACCURACY, RETENTION (ARTICLE 5)

- [ ] Apply Article 5(1) principles: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity/confidentiality, accountability (5(2))

  HIGH

- [ ] Publish a retention schedule per data category (account, billing, logs, support, marketing-consent, AI prompts)

  HIGH

- [ ] Automate purges with verifiable jobs; log each deletion run

  HIGH

- [ ] Allow users to delete account and associated data from self-service settings (fulfils Article 17 without tickets)

HIGH

## GOVERNANCE, ACCOUNTABILITY, FINES

- [ ] Maintain accountability evidence (Article 5(2) / 24): policies, training, DPIA library, ROPA, vendor list, breach log, DSAR log

  HIGH

- [ ] Apply Privacy by Design and by Default (Article 25); include a privacy checkpoint in the PR template

  HIGH

- [ ] Budget for tiered fines: up to €10M / 2% turnover (Article 83(4)); up to €20M / 4% turnover (Article 83(5))

  HIGH

- [ ] Track enforcement precedents to calibrate risk appetite

  *Meta €1.2B (DPC Ireland 2023, Schrems II SCC); Amazon €746M (CNPD 2021); WhatsApp €225M (DPC 2021); Google €50M (CNIL 2019); TikTok €345M (DPC 2023, children's data).*

- [ ] Add board-level oversight: annual privacy report on DSAR volume, breaches, DPIA backlog, vendor risk