Clinical Trials In The EU: A Compliance Checklist for GDPR & CTR Requirements

This resource is intended to support legal, clinical, and operational teams preparing to launch or expand a clinical trial in the EU, offering a checklist of recommended actions.

01

GDPR Applicability & Legal Basis

- [ ] Determine whether the GDPR applies (EU participants, EU sites, EU monitoring, EU establishment).
- [ ] Identify the GDPR lawful basis for data processing (likely public interest, legitimate interest, research, not consent).
- [ ] Identify the Article 9 condition for processing special category data (public health or scientific research).
- [ ] Appoint an EU representative if the sponsor is non-EU and no exemption applies.
- [ ] Consider appointing a DPO

02

Transparency, Notices, and Documentation

- [ ] Update the participant-facing privacy notice to reflect GDPR and CTR requirements.
- [ ] Include all mandatory transparency elements: purposes, lawful basis, transfers, DPO contact, retention, rights/limitations.
- [ ] Document how each GDPR right applies or may be restricted for research purposes.
- [ ] Maintain detailed record of processing activities (RoPA) specific to the clinical trial.

03

Informed Consent (CTR)

- [ ] Ensure the Informed Consent Form (ICF) meets CTR content requirements.
- [ ] Distinguish CTR informed consent (participation) from GDPR consent (not used as legal basis).
- [ ] Confirm whether electronic informed consent (eIC) is permitted by the Member States involved.
- [ ] Validate that information sheets and ICFs are accessible, comprehensible, and appropriately translated for each site.

04

CTIS & Regulatory Submissions

- [ ] Submit the clinical trial application via the Clinical Trials Information System (CTIS).
- [ ] Coordinate Part I (scientific) and Part II (national/ethics) assessments.
- [ ] Track deadlines, responses, and transparency obligations in CTIS.
- [ ] Prepare lay summaries and ensure timely publication as required.

05

Data Protection Impact Assessment (DPIA)

- [ ] Conduct a DPIA before trial initiation or when significant protocol changes occur.
- [ ] Assess necessity, proportionality, risks, and mitigating controls.
- [ ] Document pseudonymization and security measures (encryption, role-based access, secure transfer protocols).
- [ ] Establish a risk review process for ongoing data handling.

06

Data Protection Officer (DPO)

- [ ] Determine if appointment of a DPO is mandatory (likely for large-scale health data processing).
- [ ] If it is, ensure DPO involvement in protocol review, DPIAs, and ongoing monitoring.
- [ ] Maintain an internal register of DPO advice and follow-up actions.

07

Cross-Border Data Transfers

- [ ] Identify all data flows from the EU to the U.S. or other third countries.
- [ ] Implement appropriate transfer mechanisms (e.g., EU-U.S. Data Privacy Framework, SCCs).
- [ ] Conduct and document Transfer Impact Assessments (TIAs) where required.
- [ ] Confirm protections apply to pseudonymized data transferred to non-EU countries.

08

Site Management & Vendor Compliance

- [ ] Confirm that EU sites and laboratories implement adequate GDPR safeguards.
- [ ] Ensure Data Processing Agreements (DPAs) meet Article 28 requirements.
- [ ] Evaluate CROs, labs, and cloud vendors for GDPR and CTR compliance.
- [ ] Establish breach notification procedures aligned with Articles 33–34 GDPR.

09

Data Retention, Archiving, and Subject Rights

- [ ] Validate that retention periods comply with CTR archiving requirements.
- [ ] Apply research exemptions to erasure/restriction rights appropriately and document justification.
- [ ] Establish secure long-term storage for trial master files and subject data.
- [ ] Document how withdrawal of participation affects (or does not affect) data already collected.

Written by OGC Partner Stephan Grynwajc