EUROPEAN CLINICAL TRIALS AND THE GDPR

Data privacy considerations for life sciences organizations running clinical trials in the EU and UK

dpo centre®

Custom content for The DPO Centre by studioID

INTRODUCTION

Privacy is paramount in the EU andthe UK. And that means you as a trial sponsor must focus on safeguarding the personal data you collect on trial participants as well as vendors and even your own EU- and UK-based employees and on-site staff. Failure to do so could lead to study delays and interruptions to data flows.

EU and UK data protection laws have been around for decades. However, they've been significantly strengthened in recent years, especially with implementation of the General Data Protection Regulation (GDPR) in 2018. Most notably for clinical trial sponsors, the GDPR introduced the concept of 'extraterritorial scope', which makes organizations in any country responsible for compliance whenever EU and UK residents are involved.

As a sponsor, you're generally considered a 'data controller' (as opposed to a 'data processor') under the GDPR. That means you're required to ensure compliance with the GDPR's 7 principles (shown on the right) throughout the data collection and processing chain. Failure to comply with the GDPR could mean application delays and loss of access to study data, not to mention the possibility of fines of up to €20 million or 4% of your worldwide annual revenue.

Accountability is foundational, as it requires you to be able to demonstrate at all times how you are accountable for your compliance with the other 6 principles.

Here's how you can ensure that your trial meets GDPR requirements and that you're able to use the important personal data your trial generates.

7 principles of GDPR

GDPR focuses on these key principles:

1. Lawfulness, fairness and transparency
2. Purpose limitation
3. Data minimization
4. Accuracy
5. Storage limitation
6. Integrity and confidentiality
7. Accountability for the other 6 principles

HANDLING PERSONAL DATA OF EU AND UK TRIAL PARTICIPANTS

Perhaps nothing is as sensitive as health and medical data. That's why the GDPR classifies such data as 'special category personal data', and that's why your organization faces strict obligations around how you use it throughout its lifecycle, from collection through processing to ultimate utilization.

You are, of course, accustomed to having individuals complete informed consent forms when they join a trial. While those forms remain important, they don't give you the required consent to process the personal data you collect.

LAWFUL BASIS

The GDPR recognizes six potential lawful bases for processing personal data, three of which relate to a clinical trial: Consent, Legal Obligation and Legitimate Interests. Different aspects of a trial may require different lawful bases - here's where things can get tricky. The appropriate basis can vary depending on the country within which your trial will operate. In the UK, for example, local regulatory guidance indicates Legitimate Interests may be more appropriate than Consent.

Individual countries have their own rules you must follow, including the UK. After Brexit, the UK transposed the EU GDPR into its own laws as the UK GDPR. It complements the UK's Data Protection Act (2018) and is essentially the same, although there are a couple of notable differences.

These nuances demonstrate the critical role of the Data Protection Officer (DPO), especially if your trial spans multiple countries and/or you plan to export data outside of the EU and the UK.

> **" By having The DPO Centre take responsibility for the role of GDPR Data Protection Representative (DPR) for the PCCTC we are confident we are meeting the legal requirements of the GDPR. The initial data mapping and construction of our RoPA were a great help in understanding the practicalities of the legislation and what the consortium's obligations are."**
>
> **DREW DAVIES**
> Prostate Cancer Clinical Trials Consortium

THE CONTRACTS AND AGREEMENTS YOU'LL NEED

Accountability underpins all the principles of the GDPR. One of the ways your organization is required to demonstrate accountability is through the agreements and notices it has in place to protect personal data.

HERE ARE FIVE OF THEM:

1. Data sharing agreement: This agreement details how and why you may share data with another data controller, such as a regulator or another researcher.

2. Data processing agreement: This agreement governs the outsourcing of data processing (to your contract research organization, for example) and details their obligations when processing personal data on your behalf.

3. Privacy notice: This notice, which participants must receive before you start to collect their data (so is included within your informed consent forms), details why you're collecting the data, who you may share it with, the rights afforded to them, and how it will be retained and disposed of.

4. Joint controller agreement: If you have a joint controller (a partner research company, for example), this agreement details each party's roles and responsibilities.

5. Transfer agreements: If you plan to transfer personal data outside of the EU or the UK (even if it has been pseudonymised), a transfer agreement must be in place for most recipient countries.

" These agreements must be in place before you can begin processing or transferring personal data. That's actually a positive thing, because implementing these agreements helps your organization ensure that it has appropriate procedures in place with third parties, which will assist with the trial application process, setting up your ICFs and ethics committee reviews, and will contribute to ensuring uninterrupted data flows."

BEN SERETNY
Data Protection Officer and Head of DPOs at The DPO Centre

REQUIREMENTS FOR INTERNATIONAL DATA TRANSFERS

Complying with the GDPR takes on added complexity if you choose to export personal data on EU residents to another country. Such transfers are only permitted when appropriate safeguards are in place that mirror those mandated by the GDPR.

A few 'third countries' (non-EU states) have been awarded an 'adequacy' decision that confirms their data protection laws are 'essentially equivalent' to those of the EU. These include the UK, which is of course no longer part of the EU due to Brexit.

" As the names indicate, TIAs and TRAs assess the risks associated with transferring personal data to a third country. To conduct a thorough assessment, you should closely examine the specific laws and practices of the country in question and evaluate their potential effects on the protections provided by the GDPR."

KATRINA LEACH
Data Protection Officer and Head of DPO Operations at The DPO Centre

In North America, Canada has been awarded adequacy, however this is restricted to private Canadian organizations using the data for commercial purposes. The US was granted adequacy on 10 July 2023 with the EU-US Data Privacy Framework (DPF). This transatlantic data transfer mechanism requires US companies to self-certify compliance with the Data Privacy Framework Principles through the DPF Program website. It's worth noting that the safeguards in the Health Insurance Portability and Accountability Act (HIPAA) in the US aren't considered 'essentially equivalent' to those in the GDPR.

You can export personal data to the US by doing the following:

From the EU: Use the new Data Privacy Framework (DPF) after self-certification, or include the most recent version of the EU Commission-approved Standard Contractual Clauses (SCCs) within your transfer agreements, complemented by a transfer impact assessment (TIA)

From the UK: Complete an international data transfer agreement (IDTA), or the ICO data transfer addendum if using in combination with the EU's SCCs, along with a transfer risk assessment (TRA) or TIA as applicable.

A STREAMLINED APPROACH TO TRIAL APPROVAL

Gaining approval to conduct a trial in the EU has been simplified thanks to the Clinical Trials Regulation (CTR), which replaced the previous Clinical Trials Directive (CTD) as of 31 January 2022.

The CTR enables sponsors to submit a single application through the Clinical Trials Information System (CTIS) at euclinicaltrials.eu to seek approval to run a trial in any or all of the 30 countries that form the European Economic Area (EEA). The fully electronic process automates submission to the relevant national competent authorities and ethics committees across EEA states. Those states then collaborate on trial evaluation and supervision.

The CTIS is being gradually phased in. All new trials must now be submitted via the CTIS, while ongoing trials may continue to run until completion under the CTD. However, if they continue past 31 January 2025, they must transition to the CTIS.

“ Hundreds of trials were submitted through the CTIS even before it became mandatory, with an average time to approval of about 85 days. We look forward to seeing how the platform develops and simplifies the trial application process in the coming months and years.”

BEN SERETNY
Data Protection Officer and Head of DPOs at The DPO Centre

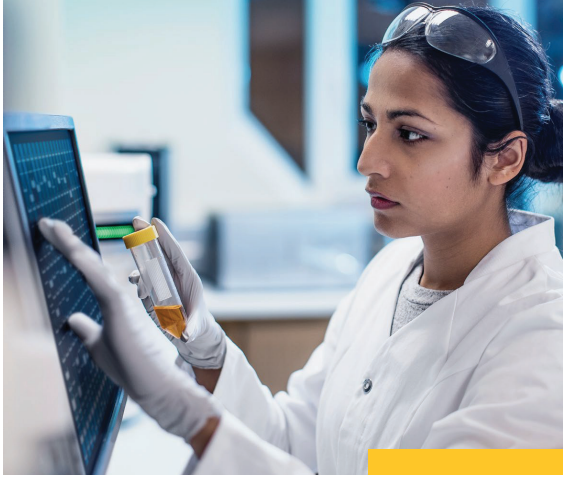
TWO KEY DATA PROTECTION ROLES: THE DPO AND THE DPR

The GDPR is complex, and the regulatory environment continues to evolve. Brexit added further complexity, as did the Schrems II decision in 2020.

The best way to enable your organization to achieve and maintain compliance is to appoint a data protection officer (DPO). This subject matter expert provides advice and guidance on the requirements of EU and UK data processing laws, from the initial trial setup and application through to the publication of data. Some sponsors appoint an in-house DPO; others rely on an outsourced DPO from an organization like The DPO Centre.

Of course, if you work with an experienced contract research organization (CRO), they should be able to demonstrate how they are GDPR compliant as a data processor. Helping you demonstrate your compliance as the data controller, however, is the job of your DPO.

If you don't have a physical presence within the European Economic Area, you must also appoint a data protection representative (DPR). This EU-based service provider acts as the point of contact for in-country data subjects and regulators.



" Trial sponsors have countless concerns, including selecting partner institutions, satisfying ethics committees, recruiting participants and processing and publishing trial data. The DPO Centre exists to assist sponsors to achieve trial success while ensuring compliance with EU and UK data protection regulations. Having worked with over 1,000 clients globally, we have an established track record of helping life sciences organizations to achieve and maintain compliance."

ROB MASSON
CEO, The DPO Centre

Data protection glossary

Navigating the GDPR means understanding an alphabet soup of terms. Here are some key terms you should know.

Clinical Trials Information System (CTIS): an online platform that allows trial sponsors to seek approval from up to 30 countries in a single application

Data protection impact assessment (DPIA): a process that helps identify and record your lawful basis for processing, to assess the impact on trial participants and to identify potential risks and mitigation strategies

Data processing agreement (DPA): an agreement that sets out the obligations of an external data processor

Data protection officer (DPO): an individual who oversees a sponsor's data protection compliance obligations

Data protection representative (DPR): an individual or organization that serves as the point of contact for EU- or UK-resident data subjects and regulators; required for sponsors based solely outside the European Economic Area (EEA)

International data transfer agreement (IDTA): an agreement that safeguards the export of data from the UK; needs to be accompanied by a transfer impact assessment (TIA)

Record of processing activities (RoPA): comprehensive documentation identifying and classifying an organization's processing of personal data

Standard Contractual Clauses (SCCs): contractual terms that provide a safeguard mechanism for exporting personal data from the EU; it must incorporate a transfer impact assessment (TIA)

Transfer impact assessment (TIA): a document that assesses the risks associated with the export of data from the EU

Transfer risk assessment (TRA): a document that assesses the risks associated with the export of data from the UK

A checklist for getting started

These questions will help your clinical trials organization ensure that you have everything in place before you begin:.

- ☐ Have you appointed your DPO?
- ☐ If required, have you appointed an EU and/or UK representative?
- ☐ Do you have the necessary contracts and agreements in place with the other parties involved, including your CRO?
- ☐ Have you ascertained the appropriate lawful bases for processing, and are these supported by the data protection authority within each jurisdiction your trial will be operating in?
- ☐ Have you completed a DPIA and mitigated the identified risks?
- ☐ Have you created privacy notices for participants, partners and employees?
- ☐ Have you trained your staff in respect of your policies and procedures?
- ☐ If relying on Consent, have you explained that consent given on an informed consent form is not the same as Consent to collect and process personal data?
- ☐ Have you considered the data protection requirements of the countries you will be operating in, especially if these include France and the UK?
- ☐ Do you understand your trial data flows and have you completed TIAs or TRAs for each relevant international data transfer?

About The DPO Centre

The DPO Centre is an EU privacy compliance consultancy and Data Protection Officer (DPO) resource centre, specializing in Life Sciences. The company delivers Data Protection Officer (DPO) and Data Protection Representative (DPR) services from its offices in London, Dublin, Amsterdam, New York, and Toronto and its network of establishments across all 27 EU Member States.

The DPO Centre provides access to one of the largest teams of experienced and permanently employed DPOs available. Since 2017, the company has delivered its services to over 1,000 clients globally, including many health, Life Sciences, MedTech, and medical device organizations.

Amsterdam · Dublin · London · New York · Toronto
+44 (0) 203 797 1289
hello@dpocentre.com
www.dpocentre.com

04-2025